Cyber Threat Advisory

NOVEMBER 2023

Contents

Monthly Highlights	1
Ransomware Tracker	3
Over 10,000 Cisco Devices Hacked in IOS XE Zero-Day Attacks	4
Hackers Hijack Citrix NetScaler Login Pages to Steal Credentials	5
GNOME Linux Systems Exposed to RCE Attacks via File Downloads	7
FBI, CISA Warn of Rising AvosLocker Ransomware Attacks Against Critical Infrastructure	8
Top Threat Actors	9
Top Exploited Vulnerabilities	9-10
Security Bulletin	10
Reference Links	14

Monthly Highlights - November

1. **Shadow Silent on Data Breach as Hacked Data Appears Genuine** – The scale of the data breach at the French cloud gaming provider Shadow appears to be more extensive than initially acknowledged by the company, as indicated by a sample of the stolen data scrutinized by TechCrunch. In an e-mail dispatched to affected customers this week, Shadow's CEO, Eric Sèle, disclosed that a hacker executed a sophisticated social engineering attack targeting one of the company's employees, leading to unauthorized access to sensitive customer information. This encompassed complete names, e-mail addresses, dates of birth, billing addresses, and credit card expiration dates.

   TechCrunch has gained access to a sample of the purloined data, which comprises 10,000 distinct records, shared by the individual claiming responsibility for the cyberattack. The hacker, who revealed the breach on a prominent hacking forum, asserts to have breached the data of over 530,000 shadow customers and is currently offering this data for sale, alleging that they were deliberately ignored by the company.

   Within the data that has been examined, numerous customer billing addresses align with their private residential addresses. The dataset also encompasses private API keys linked to customer accounts, though it remains uncertain whether these keys are accessible by customers. Additionally, non-personal information concerning customer accounts, such as subscription status and account blacklisting, is present in the dataset.

   Based on the most recent record of the stolen data, it appears that Shadow's security was compromised on or shortly after September 28. In an e-mail dispatched to those impacted by the incident, which has not been officially published on Shadow's website or shared on the company's social media

platforms, Shadow disclosed that the breach transpired “at the end of September” when an employee downloaded a malware-infected Steam game via Discord.

When contacted for a response, a spokesperson for Shadow, Thomas Beaufils, refrained from providing a statement but did not challenge the reported findings. It remains uncertain whether Shadow has informed France’s data protection regulator, CNIL, about the breach, as required under European law. A request for comment submitted to a CNIL spokesperson has not been immediately answered.

2. **Microsoft to Phase Out NTLM in Favor of Kerberos for Stronger Authentication** – Microsoft has announced its intention to phase out the use of NT LAN Manager (NTLM) in Windows 11 as part of its efforts to enhance authentication methods and improve security. The company is shifting its focus towards strengthening the Kerberos authentication protocol, which has been the default since year 2000, while reducing reliance on NTLM.

   The upcoming features for Windows 11 include Initial and Pass-Through Authentication Using Kerberos (IAKerb) and a local Key Distribution Center (KDC) for Kerberos. IAKerb allows clients to authenticate with Kerberos across various network topologies, while the local KDC extends Kerberos support to local accounts.

   NTLM and Kerberos differ in how they manage authentication. NTLM uses a three-way handshake between the client and server, while Kerberos employs a two-part process involving a ticket-granting service or key distribution center. Additionally, NTLM relies on password hashing, whereas Kerberos uses encryption.

   NTLM has been plagued by security weaknesses, including vulnerabilities to relay attacks, which could enable unauthorized access to network resources. Microsoft is actively addressing hardcoded NTLM instances in its components in preparation for the eventual removal of NTLM in Windows 11. The company is making improvements to promote the use of Kerberos over NTLM. Microsoft intends to enable these changes by default, requiring little to no configuration for most scenarios. NTLM will still be available as a fallback for compatibility with existing systems.

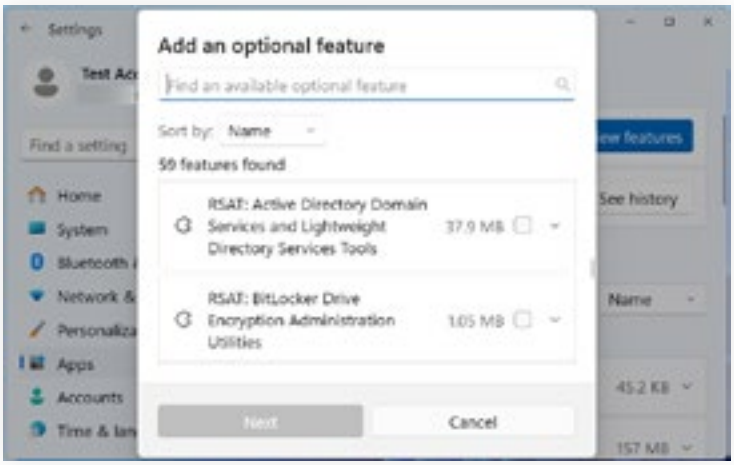
   In a separate context, it’s important to note that a device under the attacker’s control was added to the targeted employee’s Okta account after the attacker produced a deepfake of an employee’s voice and convinced an IT team member to provide an additional MFA code.

3. **Microsoft to Kill Off VBScript in Windows to Block Malware Delivery** – Microsoft is preparing to phase out VBScript in forthcoming Windows releases, marking the end of a three-decade period during which it served as an integral part of the Windows ecosystem. VBScript will transition into an on-demand point before eventually being removed.

   VBScript, which has been bundled with Internet Explorer and has been necessary in easing active scripting within Windows surroundings and communication with host operations via Windows Script, is now being disapproved. Microsoft blazoned,” In future Windows releases, VBScript will be available as a point on demand before its removal from the operating system.”

   To ensure a smooth transition, the VBScript point on demand will be originally preinstalled, allowing for continued operation while preparing for its withdrawal. This approach aligns with the Features on Demand (FODs) conception, which offers voluntary factors within the Windows operating system, similar as the. NET Framework (. NetFx3), Hyper-V, and the Windows Subsystem for Linux. These factors aren’t installed by default but can be added as demanded.

   Microsoft took way to disable VBScript by defalult in Internet Explorer 11 on Windows 10 with the July 2019 Patch Tuesday cumulative updates. This decision is part of a broader strategy aimed at reducing the threat of malware juggernauts exploiting various Windows and Office features for the purpose of infecting systems.



Windows 11 optional features user interface

4. **Over 17,000 WordPress Sites Hacked in Balada Injector Attacks Last Month** – Balada Injector is a significant cyber operation that came to light in December 2022 when Dr. Web discovered it. This operation has been exploiting known vulnerabilities in WordPress plugins and themes to inject a Linux backdoor. The purpose of this backdoor is to redirect

visitors of compromised websites to fake tech support pages, fraudulent lottery win offers, and push notification scams. It is likely that this operation is part of scam campaigns or is being offered as a service to scammers. In April 2023, Sucuri reported that Balada Injector has been active since 2017 and has compromised nearly one million WordPress sites. Sucuri identified six distinct attack waves, some of which have variants:

1. The initial wave involved compromising WordPress sites by injecting malicious scripts from stay.decentralappps[.]com, impacting over 5,000 sites with two variants (4,000 and 1,000).
2. Attackers used a malicious script to create rogue WordPress administrator accounts. Initially, a 'greeceman' username was used, but the attackers switched to auto-generated usernames based on the site's hostname.
3. The third wave saw the abuse of WordPress's theme editor to embed backdoors in the Newspaper theme's 404.php file for stealthy persistence.
4. Attackers then switched to installing the wp-zexit plugin, mimicking WordPress admin behaviour and hiding the backdoor in the website's Ajax interface.
5. In the fifth wave, attackers introduced three new domains and increased randomization across injected scripts, URLs, and codes, making tracking and detection more challenging. One specific injection from this wave was detected in 484 sites.
6. The latest attacks employ promsmotion[.]com subdomains instead of stay.decentralappps[.]com, limiting deployment to three specific injections detected in 92, 76, and 67 websites. Sucuri's scanner has identified the promsmotion injections on a total of 560 sites.

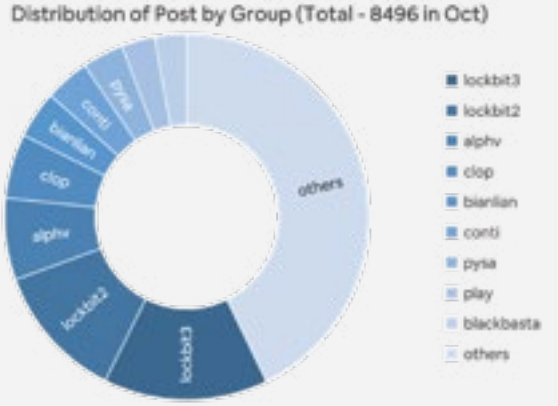
As of September 2023, Sucuri detected Balada Injector on over 17,000 WordPress sites, with more than half (9,000) compromised through the exploitation of CVE-2023-3169. The swift optimization of these attack waves suggests that the threat actors behind Balada Injector can adapt their techniques rapidly to maximize their impact. To defend against Balada Injector, it is recommended to upgrade the tagDiv Composer plugin to version 4.2 or later, which addresses the mentioned vulnerability.

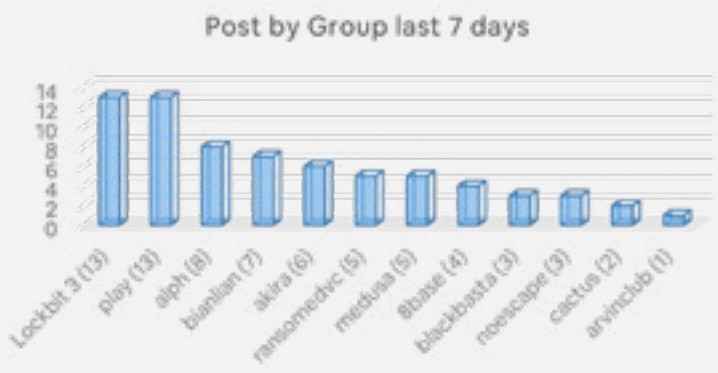
5. **Security Patch for Two New Flaws in Curl Library Arriving on October 11** – The maintainers of the Curl library have issued a security advisory warning of two vulnerabilities set to be addressed in an upcoming update scheduled for release on October 11, 2023. These vulnerabilities include one of high severity (CVE-2023-38545) and one of low severity (CVE-2023-38546). Specific details about these vulnerabilities and the affected version ranges have not been disclosed to prevent potential pre-release exploitation.

   Curl, powered by libcurl, is a widely used command-line tool for data transfer using URL syntax. It supports numerous protocols, including FTP(S), HTTP(S), IMAP(S), LDAP(S), MQTT, POP3, RTMP(S), SCP, SFTP, SMB(S), SMTP(S), TELNET, WS, and WSS. While CVE-2023-38545 impacts both libcurl and curl, CVE-2023-38546 affects only libcurl.

   It's crucial for organizations to stay proactive in securing their systems. Saeed Abbasi, a product manager at Qualys Threat Research Unit (TRU), mentioned that "with specific version range details undisclosed to prevent pre-release problem identification, the vulnerabilities will be fixed in curl version 8.4.0." Abbasi also advised organizations to take swift action by inventorying and scanning all systems utilizing curl and libcurl. This will help in identifying potentially vulnerable versions once the details are revealed upon the release of Curl 8.4.0 on October 11.

Ransomware Tracker





Over 10,000 Cisco Devices Hacked in IOS XE Zero-Day Attacks

In the context of researching CVE-2023-20198 attacks, Orange Cyberdefense CERT found that over 34.5K Cisco IOS XE devices were hacked.

Attackers have compromised and introduced damaging implants into over 10,000 Cisco IOS XE devices by taking advantage of a recently discovered zero-day issue.

Enterprise switches, aggregation and industrial routers, access points, wireless controllers, and more are included in the list of products running the Cisco IOS XE software.

Threat intelligence firm VulnCheck claims that Cisco IOS XE systems that have the Web User Interface (Web UI) feature enabled and the HTTP or HTTPS Server features toggled on have been extensively exploited in attacks because of the highest severity vulnerability (CVE-2023-20198).

Detection

Cisco revealed that an unauthorized attacker can remotely take over impacted Cisco routers and switches and obtain full administrator capabilities by taking advantage of the IOS XE zero-day vulnerability.

Until a patch is released, the business advised administrators to turn off the vulnerable HTTP server capability on all systems that are connected to the internet.

After receiving reports of odd behavior on a customer device, Cisco's Technical Assistance Centre (TAC) identified the CVE-2023-20198 attacks in late September. The attacks were first noted on September 18, when the attackers were seen setting up the local user accounts "cisco_tac_admin" and "cisco_support."

Additionally, the attackers used CVE-2021-1435 exploits and other unidentified techniques to deploy malicious implants that allowed them to run arbitrary commands at the system or IOS levels on devices that were hacked.

> **Over 140,000 Cisco devices that enabled the Web UI are currently visible in a Shodan search for those devices.**

We conclude that the same actor most likely carried out these activity clusters. The two clusters seemed to be near each other, and the October steps looked to expand upon the September activity.

The October activity shows the actor expanding their operation to include establishing persistent access via implant deployment, whereas the first cluster may represent the actor's first attempt and code testing.

Prevention

- Block unknown scripts from running.
- Patch all DLL & script files in production.
- Do not click on malicious links.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP & SSH 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 mechanisms through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.

Remediation

- Monitor event logs.
- Regularly back up data and store backups offline
- Enable automatic software updates on computers
- Administrators should limit port proxy usage within environments.
- Download only trusted software from known sites.
- Use post method for sending & retrieving data through communication channels.
- Update your machine & servers on a monthly basis.
- Enable packet filtration through the firewall.
- Configure DLP in environment properly.
- Update the operating system (OS) and all installed programs.
- Use a paid VPN to access web applications or networks.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

Hackers Hijack Citrix NetScaler Login Pages to Steal Credentials

A large campaign has been launched by hackers to obtain user credentials by taking advantage of the recently discovered CVE-2023-3519 vulnerability in Citrix NetScaler Gateways.

Citrix NetScaler ADC and NetScaler Gateway are affected by a critical unauthenticated remote code execution vulnerability that was identified as a zero-day in July.

More than 640 Citrix servers had been compromised by early August, and by mid-August, the total number had increased to 2,000.

The attack surface for Citrix devices remains significant according to IBM's X-Force, and in September, hackers started using CVE-2023-3519 to inject JavaScript that captures login credentials despite the repeated recommendations to update Citrix equipment.

Detection

An investigation of a case involving a client who noticed weak authentications on their NetScaler device led X-Force to identify the Netscaler credential-stealing campaign.

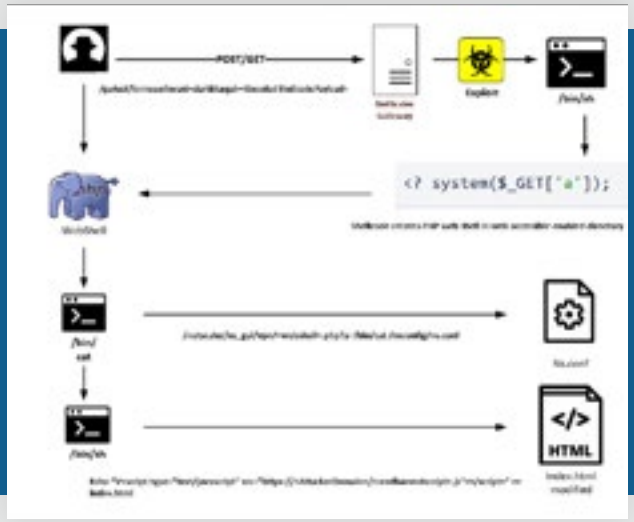
During the investigation, the responders discovered that a malicious JavaScript script capable of stealing credentials was injected into the index.html login page of a Citrix NetScaler device by hackers applying CVE-2023-3519.

Starting with a web request, the attack takes advantage of NetScaler devices that are vulnerable to create a basic PHP web shell on "/netscaler/ns_gui/vpn."

The attackers can connect to the compromised endpoint in real time with this web shell, which they utilize to gather configuration information from the "ns.conf" file.

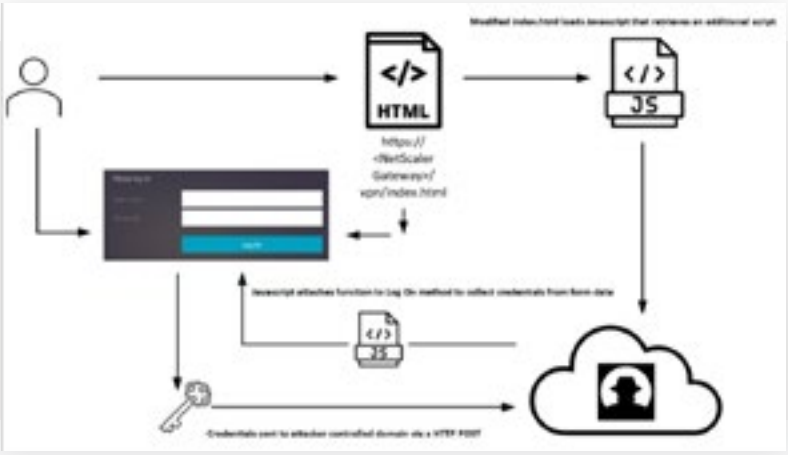
Subsequently, the hackers add their personal HTML code to the "index.html" page, referencing a remote JavaScript file that then obtains and runs more JS code.

> **The final piece of code in JS is meant to collect credentials by adding a special function to the "Log On" button on the VPN authentication page.**



The final piece of code in JS is meant to collect credentials by adding a special function to the "Log On" button on the VPN authentication page.

Ultimately, an HTTP POST request is used to exfiltrate the obtained credentials to the attackers.



During this campaign, the threat actor registered multiple domains, including cloudjs[.]live, jscloud[.]ink, jscloud[.]live, jscloud[.]biz, and jscdn[.]biz.

X-Force found nearly 600 distinct IP addresses for NetScaler devices whose login pages had been altered to aid in the credential-stealing operation.

Although hacked systems can be found anywhere in the world, most victims are in the US and Europe.

Prevention

- Block unknown scripts from running.
- Do not click on malicious links.
- 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 mechanisms through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.

Remediation

- Monitor event logs.
- Administrators should limit port proxy usage within environments.
- Download only trusted software from known sites.
- Use post method for sending & retrieving data through communication channels.
- Update your machine & servers on a monthly basis.
- Enable packet filtration through the firewall.
- Configure DLP in environment properly.
- Update the operating system (OS) and all installed programs.
- Use a paid VPN to access web applications or networks.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

Image Source

GNOME Linux Systems Exposed to RCE Attacks via File Downloads

An attacker can run arbitrary code on Linux computers using the GNOME desktop environment by taking advantage of a memory corruption vulnerability in the open-source libcue library.

The Tracker Miners file metadata indexer, installed by default in the most recent GNOME releases, incorporates libcue—a library to handle cue sheet files.

Cue sheets, also referred to as CUE files, are simply text files that list the length, song title, artist, and other information about the arrangement of audio tracks on a CD. They are commonly used together with FLAC audio files.

The vulnerability (CVE-2023-43641) allows attackers to successfully execute malicious code by using Tracker Miners to automatically index all files that are downloaded to refresh the search index on GNOME Linux systems.

GNOME is a popular desktop environment that may be found in many different Linux distributions, including Fedora, Ubuntu, Debian, Red Hat Enterprise, and SUSE Linux Enterprise.

Detection

The targeted user needs to download a maliciously created .CUE file, which is subsequently kept in the ~/Downloads folder to take use of this vulnerability.

When the Tracker Miners metadata indexer automatically parses the stored file through the tracker-extract procedure, a memory corruption vulnerability is triggered.

Researchers found that all it takes for an attacker to exploit CVE-2023-43641 and execute code on your computer is for you to unintentionally click a malicious link.

Researchers tweeted a video and demonstrated a proof-of-concept exploit. To give all GNOME users time to update and safeguard their systems, the PoC release has been rescheduled.

CLICK TO WATCH

Although the proof-of-concept exploit must be adjusted to function well for every Linux distribution, the researcher claimed to have already developed “very reliable” exploits for Fedora 38 and Ubuntu 23.04.

Although CVE-2023-43641 can only be successfully exploited by tricking a potential victim into downloading a .cue file, executives are advised to patch their systems and reduce the risks associated with this security flaw, as it allows for code execution on devices running the most recent versions of popular Linux distributions, such as Fedora, Ubuntu, and Debian.

Researchers have discovered other serious security holes in Linux in recent years. These include a problem that allows privilege escalation in the GNOME Display Manager (gdm) and a way to bypass authentication in the polkit auth system service, which is installed by default on a lot of contemporary Linux machines.

Prevention

- Block unknown scripts from running.
- Do not click on malicious links.
- 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 mechanisms through the firewall.
- Enable limitations on administrative access or rights.

Remediation

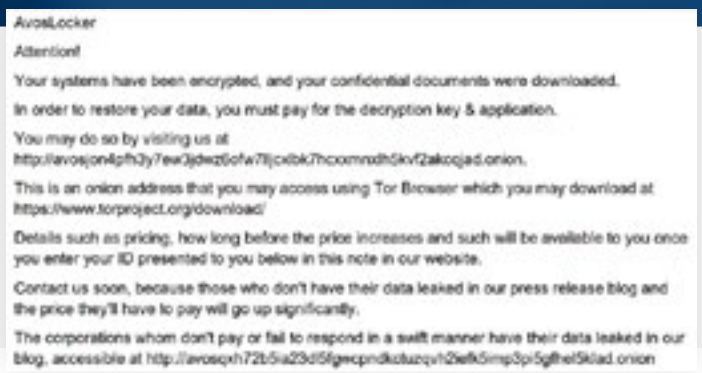
- Monitor event logs.
- Administrators should limit port proxy usage within environments.
- Download only trusted software from known sites.
- Use post method for sending & retrieving data through communication channels.
- Update your machine & servers on a monthly basis.
- Enable packet filtration through the firewall.
- Configure DLP in environment properly.
- Update the operating system (OS) and all installed programs.
- Use a paid VPN to access web applications or networks.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

FBI, CISA Warn of Rising AvosLocker Ransomware Attacks Against Critical Infrastructure

The U.S. government has added open-source utilities, customized PowerShell scripts, and batch files to the list of tools used by AvosLocker ransomware affiliates in their attacks.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have collaborated on a cybersecurity warning where they have shared a YARA rule for identifying malware that appears as a valid network monitoring tool.

> **According to the agencies, AvosLocker affiliates use open-source remote system administration tools and legal software to breach organizations' networks. Followers of AvosLocker then use data extortion techniques based on exfiltration, threatening to disclose and/or publish stolen information.**


AvosLocker

Attention!

Your systems have been encrypted, and your confidential documents were downloaded.

In order to restore your data, you must pay for the decryption key & application.

You may do so by visiting us at
http://avosjon4pfh3y7ew3jdwz6ofw7ltjcxbk7hcxxmnxdh5kvf2akcqjad.onion.

This is an onion address that you may access using Tor Browser which you may download at
https://www.torproject.org/download/

Details such as pricing, how long before the price increases and such will be available to you once you enter your ID presented to you below in this note in our website.

Contact us soon, because those who don't have their data leaked in our press release blog and the price they'll have to pay will go up significantly.

The corporations whom don't pay or fail to respond in a swift manner have their data leaked in our blog, accessible at http://avosqxh72b5a23d5fgecpndkzluzquh2wfk5rnp3pi5gfhel5klad.onion

Detection

Affiliates of the AvosLocker ransomware are known to breach and steal data from business networks using open-source code and legal tools for remote system management.

The FBI saw the threat actors proceeding laterally on the network, gaining additional privileges, and disabling security agents on the systems by using web shells, batch scripts, and custom PowerShell.

The government officials share the following devices in the new advice as being a part of the AvosLocker ransomware affiliates' toolkit:

- Backdoor Access tools like: Splashtop Streamer, Tactical RMM, PuTTy, AnyDesk, PDQ Deploy, Atera Agent
- Open-source network tunnelling utilities: Ligolo, Chisel
- Adversary emulation frameworks Cobalt Strike and Sliver for command and control
- Lazagne and Mimikatz for harvesting credentials
- FileZilla and Rclone for data exfiltration

Additional freely accessible programs found in AvosLocker attacks are 7zip, RDP Scanner, and Notepad++. There were also authentic native Windows tools shown, such as PsExec and Nltest.

A virus known as NetMonitor.exe, which poses as a legitimate process and "has the appearance of a real-life network monitoring tool," is another element of AvosLocker attacks.

Despite its appearance, NetMonitor, a persistence tool, emerges from the network every five minutes and serves as a reverse proxy, allowing the threat actors to connect remotely to the compromised network.

> **Utilizing information from "an advanced digital forensics group's" research, the FBI developed the YARA rule listed below to identify NetMonitor malware on a network.**

```
rule NetMonitor
{
  meta:
    author = "FBI"
    source = "FBI"
    sharing = "TLP:CLEAR"
    status = "RELEASED"
    description = "Yara rule to detect NetMonitor.exe"
    category = "MALWARE"
    creation_date = "2023-05-05"
  strings:
    $rc4key = {11 4b 8c dd 65 74 22 c3}
    $op0 = {c6 [3] 00 00 05 c6 [3] 00 00 07 83 [3] 00 00 05 0f 85 [4] 83 [3] 00 00
01 75 ?? 8b [2] 4c 8d [2] 4c 8d [3] 00 00 48 8d [3] 00 00 48 8d [3] 00 00 48 89
[3] 48 89 ?? e8}
  condition:
    uint16(0) == 0x5A4D
    and filesize < 50000
    and any of them
}
```

Prevention

- Block unknown scripts from running.
- Do not click on malicious links.
- Apply filter to accept only trusted HTTPS connections.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the communication 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 mechanisms through the firewall.
- Enable limitations on administrative access or rights.

Remediation

- Monitor event logs.
- Administrators should limit port proxy usage within environments.
- Download only trusted software from known sites.
- Use post method for sending & retrieving data through communication channels.
- Update your machine & servers on a monthly basis.
- Enable packet filtration through the firewall.
- Configure DLP in environment properly.
- Update the operating system (OS) and all installed programs.
- Use a paid VPN to access web applications or networks.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

TOP THREAT ACTORS

Threat Actor	IOC Reference
BlackTech APT	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a
Shadow Syndicate	https://www.group-ib.com/blog/shadowsyndicate-raas/
UNC3944	https://www.mandiant.com/resources/blog/unc3944-sms-phishing-sim-swapping-ransomware

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
SolarWinds Access Rights Manager OpenClientUpdateFile Directory Traversal Remote Code Execution Vulnerability CVE-2023-35187	Vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Access Rights Manager. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations.	https://securityaffairs.com/152873/security/solarwinds-access-rights-manager-rces.html#google_vignette
NI Measurement & Automation Explorer Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-4601	Vulnerability allows remote attackers to execute arbitrary code on affected installations of NI Measurement & Automation Explorer. 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.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2023-4601
SolarWinds Access Rights Manager IFormTemplate Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2023-35180	Vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Access Rights Manager. The specific flaw exists within the deserialization of JSON data sent to the API via TCP port 443.	https://socradar.io/solarwinds-releases-crucial-fixes-for-arm-security-vulnerabilities-cve-2023-35182-cve-2023-35185-and-cve-2023-35187/
F5 BIG-IP OS unzip Directory Traversal Remote Code Execution Vulnerability CVE-2023-41373	Vulnerability allows remote attackers to execute arbitrary code on affected installations of F5 BIG-IP OS. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations.	https://my.f5.com/manage/s/article/K000135689
Microsoft Windows DirectX GpuMmu Race Condition Local Privilege Escalation Vulnerability CVE-2023-38159	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38159
Magnet Forensics AXIOM Command Injection Remote Code Execution Vulnerability CVE-2023-42128	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Magnet Forensics AXIOM. User interaction is required to exploit this vulnerability in that the target must acquire data from a malicious mobile device.	https://www.cybersecurity-help.cz/vdb/SB2023100903

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
Zero-day D-Link D-View coreservice_action_script Exposed Dangerous Function Remote Code Execution Vulnerability CVE-2023-44414	Vulnerability allows remote attackers to execute arbitrary code on affected installations of D-Link D-View. The specific flaw exists within the coreservice_action_script action.	https://www.cybersecurity-help.cz/vdb/SB2023100540
Apple Safari TypedArray copyWithin Integer Underflow Remote Code Execution Vulnerability CVE-2023-38600	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Apple Safari. 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://access.redhat.com/security/cve/cve-2023-38600
A10 Thunder ADC FileMgmtExport Directory Traversal Arbitrary File Read and Deletion Vulnerability CVE-2023-42130	Vulnerability allows remote attackers to read and delete arbitrary files on affected installations of A10 Thunder ADC. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations.	https://www.cybersecurity-help.cz/vdb/SB2023100513
Apple iTunes Incorrect Permission Assignment Privilege Escalation Vulnerability CVE-2022-26773	Vulnerability allows local attackers to escalate privileges on affected installations of Apple iTunes. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://support.apple.com/en-us/HT213259
ManageEngine ADManager Plus installServiceWithCredentials Command Injection Remote Code Execution Vulnerability CVE-2023-38743	Vulnerability allows remote attackers to execute arbitrary code on affected installations of ManageEngine ADManager Plus. The specific flaw exists within the installServiceWithCredentials function. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call.	https://petrusviet.medium.com/cve-2023-38743-manageengine-admanager-command-injection-6afccbb196fe
Linux Kernel eBPF Improper Input Validation Privilege Escalation Vulnerability CVE-2023-39191	Vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel. An attacker must first obtain the ability to execute high-privileged code on the target system to exploit this vulnerability.	https://access.redhat.com/security/cve/cve-2023-39191
Zero-Day Control Web Panel Missing Authentication Remote Code Execution Vulnerability CVE-2023-42121	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Control Web Panel. An attacker can leverage this vulnerability to execute code in the context of a valid CWP user.	https://securityonline.info/cve-2023-42121-critical-control-web-panel-rce-vulnerability/
Cacti graph_view SQL Injection Authentication Bypass Vulnerability CVE-2023-39365	Vulnerability allows remote attackers to bypass authentication or escalate privileges on affected installations of Cacti. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries.	https://ubuntu.com/security/CVE-2023-39365
Zero-Day D-Link DIR-X3260 prog.cgi Incorrect Implementation of Authentication Algorithm Authentication Bypass Vulnerability CVE-2023-44420	Vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-X3260 routers. The issue results from an incorrect implementation of the authentication algorithm.	https://vuldb.com/?id.241373
Delta Electronics DIAEnergie HandlerUploadCalendar Use of Hard-Coded Credentials Authentication Bypass Vulnerability CVE-2022-3214	Vulnerability allows remote attackers to bypass authentication on affected installations of Delta Electronics DIAEnergie. The specific flaw exists within the processing of requests to the HandlerUploadCalendar endpoint.	https://cert.civis.net/en/index.php?action=alert&param=CVE-2022-3214
Microsoft PC Manager SAS Token Incorrect Permission Assignment Authentication Bypass Vulnerability	Vulnerability allows remote attackers to bypass authentication on Microsoft PC Manager. The specific flaw exists within the permissions granted to an SAS token.	https://www.zerodayinitiative.com/advisories/ZDI-23-1528/

Security Bulletin

1. **Researchers Unveil ToddyCat's New Set of Tools for Data Exfiltration –** The advanced persistent threat (APT) actor known as ToddyCat has been connected to a new set of malicious tools that are designed for information exfiltration, providing a deeper understanding of the hacking crew's strategies and capabilities.

   The discoveries come from Kaspersky, which shed light on the adversary last year, connecting it to attacks made against high-profile entities in Europe and Asia for about three years.

While the group's arsenal prominently features Ninja Trojan and a backdoor called Samurai, further investigation has revealed a whole new set of malicious software created and maintained by the threat actor to achieve persistence, conduct file operations, and load additional payloads at runtime.

This comprises a collection of loaders that comes with capabilities to dispatch the Ninja Trojan as a second stage, a tool called LoFiSe to discover and collect files of interest, a DropBox uploader to save stolen data to Dropbox, and Pcexter to exfiltrate archive files to Microsoft OneDrive.

ToddyCat has been seen utilizing custom scripts for data collection. They use an inactive backdoor that receives commands with UDP bundles, Cobalt Strike for post-exploitation, and compromised admin credentials to facilitate lateral movement to pursue their malicious activities.

"We observed script variations designed exclusively to gather data and copy files to specific folders, but without including them in compressed archives," Kaspersky said.

"In these cases, the actor executed the script on the remote host using the standard remote task execution technique. The collected files were then manually transferred to the exfiltration host using the xcopy utility and lastly compressed using the 7z binary."

The disclosure comes as Check Point uncovered that multiple government and telecom entities in Asia have been targeted as part of an ongoing campaign since 2021 employing a wide assortment of "disposable" malware to evade detection and deliver next-stage malware.

2. **DarkGate Malware Spreading via Messaging Services Posing as PDF Files –** It has been noted that the malware known as DarkGate is spreading through instant messaging services like Microsoft Teams and Skype.

   In these attacks, a loader script for Visual Basic for Applications (VBA) is delivered through messaging apps in the guise of a PDF document. When the PDF is read, an AutoIt script that launches malware is downloaded and executed.

   "It's unclear how the originating accounts of the instant messaging applications were compromised; however, it is hypothesized to be either through leaked credentials available through underground forums or the previous compromise of the parent organization," Trend Micro stated in a fresh analysis released Thursday.

   DarkGate is a commodity malware that was originally discovered by Fortinet in November 2018. It has many characteristics that enable it to mine bitcoin, collect sensitive data from web browsers, and provide its operators with remote control over the compromised systems. It can also be used to download extra payloads, like Remcos RAT.

   To trick unsuspecting users into installing the malware, social engineering efforts that use search engine optimization (SEO) poisoning and phishing emails have become more prevalent in recent months.

   The spike coincides with the malware author's decision, after years of private use, to market the program on dark web forums and offer it for hire as malware-as-a-service to other threat actors.

   Truesec first brought attention to the use of Microsoft Teams chat messages as a DarkGate transmission vector early last month, suggesting that many threat actors are probably using them.

   According to Trend Micro, the Americas have seen the greatest number of attacks, closely followed by Asia, the Middle East, and then Africa.

   Except for the altered initial access route, the entire infection process that is abusing Teams and Skype closely mirrors a malspam campaign that Telekom Security identified in late August 2023.

   Trend Micro researchers Trent Bessell, Ryan Maglaque, Aira Marcelo, Jack Walsh, and David Walsh stated that "the threat actor exploited a trusted relationship between the two organizations to deceive the recipient into executing the attached VBA script. Access to the victim's Skype account allowed the actor to hijack an existing messaging thread and craft the naming convention of the files to relate to the context of the chat history."

   The legitimate AutoIt application (AutoIt3.exe) and the related AutoIT script that starts the DarkGate malware are retrieved via the VBA script.

   In a different attack sequence, the attackers send a Microsoft Teams message with a ZIP archive attachment that contains an LNK file. This file is meant to launch a VBA script that will extract the DarkGate artifact and AutoIt3.exe.

   "Cybercriminals can use these payloads to infect systems with various types of malwares, including info stealers, ransomware, malicious and/or abused remote management tools, and cryptocurrency miners," according to the researchers.

   "As long as external messaging is allowed, or abuse of trusted relationships via compromised accounts is unchecked, then this

technique for initial entry can be done to and with any instant messaging (IM) apps."

New Magecart Campaign Alters 404 Error Pages to Steal Shoppers' Credit Cards – In what has been called the latest evolution of the attacks, a sophisticated Magecart campaign has been observed manipulating websites' default 404 error page to conceal malicious code.

According to Akamai, the activity targets WooCommerce and Magento websites; some of the victims are major corporations in the retail and food sectors.

Roman Lvovsky, a security researcher at Akamai, stated in a Monday analysis that "in this campaign, all the victim websites we detected were directly exploited, as the malicious code snippet was injected into one of their first-party resources."

This entails either directly inserting the code into the HTML pages or placing it inside a first-party script that was loaded with the website.

The loader code retrieves the main payload during runtime to obtain the sensitive data entered by users on checkout pages and exfiltrate it to a remote server. This multi-stage chain allows the attacks to be executed.

"The purpose of separating the attack into three parts is to conceal the attack in a way that makes it more challenging to detect," Lvovsky said. "This makes the attack more discreet and more difficult to detect by security services and external scanning tools that might be in place on the targeted website."

"This allows for the activation of the full flow of the attack only on the specifically targeted pages; that is, because of the obfuscation measures used by the attacker, the activation of the full attack flow can only occur where the attacker intended for it to execute."

The use of 404 error pages is one of the three variations of the campaign, the other two of which obfuscate the skimmer code in a malformed HTML image tag's onerror attribute and as an inline script that masquerades as the Meta Pixel code snippet.

The phony Meta Pixel code retrieves a PNG image from the website's own directory and appends a Base64-encoded string to the end of the image binary file. Upon decoding, this string reveals a segment of JavaScript code that connects to a domain controlled by the actor to obtain the second stage payload.

"This code is responsible for carrying out various malicious activities on the targeted sensitive page, with the goals of reading the user's sensitive personal and credit card data and transmitting it back to the skimmer's C2 server," Lvovsky stated.

These two methods are intended to evade security controls like external scanning and static analysis, thereby extending the attack chain's lifespan.

The third loader variant, on the other hand, is notable for using the default error page on the intended website as part of an inventive concealment strategy. It appears as a fake Meta Pixel code or an inline script and sends a GET request to a URL that does not exist on the website, resulting in a "404 Not Found" error.

This answer refers to an altered error page that conceals the skimmer code. To collect data for later exfiltration in the form of a Base64-encoded string, the skimmer overlays a lookalike payment form on checkout pages.

"The idea of manipulating the default 404 error page of a targeted website can offer Magecart actors various creative options for improved hiding and evasion," Lvovsky stated.

"The request to the first-party path leading to the 404 page is another evasion technique that can bypass Content Security Policy headers and other security measures that may be actively analyzing network requests on the page."

3. **CERT-UA Reports: 11 Ukrainian Telecom Providers Hit by Cyberattacks –** Between May and September 2023, threat actors "interfered" with at least 11 telecommunication service providers in Ukraine, according to the Computer Emergency Response Team of Ukraine (CERT-UA).

   Customers' services were interrupted because of the intrusions, according to the agency, which is monitoring the activity under the code UAC-0165.

   The attacks begin with a reconnaissance phase, during which the network of a telecom company is scanned to find potential entry points and exposed RDP or SSH interfaces.

   "It should be noted that reconnaissance and exploitation activities are carried out from previously compromised servers located, in particular, in the Ukrainian segment of the internet," stated CERT-UA. "To route traffic through such nodes, Dante, SOCKS5, and other proxy servers are used."

   The employment of two specialized programs, POEMGATE and POSEIDON, which permit credential theft and remote control of the compromised hosts, makes the attacks noteworthy. A program called WHITECAT is used to remove the forensic trail. Furthermore,

regular VPN accounts without multi-factor authentication are used to gain persistent unauthorized access to the provider's infrastructure.

After a successful breach, attempts are made to disable data storage systems along with servers, and network equipment, particularly Mikrotik equipment.

This development coincides with the agency's announcement that, during the first week of October 2023, it detected four phishing waves executed by hackers—identified as UAC-0006 group—who were using the SmokeLoader malware.

"Legitimate compromised email addresses are used to send emails, and SmokeLoader is delivered to PCs in several ways," said CERT-UA.

"The attackers' intention is to attack accountants' computers in order to steal authentication data (login, password, key/certificate) and/or change the details of financial documents in remote banking systems in order to send unauthorized payments."

4. **Gaza-Linked Cyber Threat Actor Targets Israeli Energy and Defense Sectors –** A string of cyberattacks targeting Israeli private sector energy, defense, and telecommunications companies have been traced back to a threat actor based in Gaza.

   Microsoft is monitoring the campaign under the codename Storm-1133; the company disclosed information about it in its fourth annual Digital Defense Report.

   "We assess this group works to further the interests of Hamas, a Sunni militant group that is the de facto governing authority in the Gaza Strip, as activity attributed to it has largely affected organizations perceived as hostile to Hamas," the business stated.

   The campaign's targets included groups that supported Fatah, a Palestinian nationalist and social democratic political party with its headquarters in the West Bank, as well as organizations in the Israeli energy and defense sectors.

   Attack chains use a combination of social engineering and fictitious LinkedIn profiles, posing as Israeli software developers, project managers, and HR directors, to contact and send phishing messages, carry out reconnaissance, and infect employees with malware.

   Microsoft reported that it had also seen Storm-1133 trying to get inside other groups that were publicly connected to Israeli targets of interest.

   Along with a configuration that enables the group to dynamically update the command-and-control (C2) infrastructure hosted on Google Drive, these intrusions are made to deploy backdoors.

   "This technique enables operators to stay a step ahead of certain static network-based defense," Redmond stated.

   The revelation coincides with a worsening of the Israeli-Palestinian conflict and a rise in hostile hacktivist campaigns like Ghosts of Palestine, which try to take down Israeli, American, and Indian government websites and IT infrastructure.

   Falconfeeds.io stated in a post shared on X (formerly Twitter) that there have been "around 70 incidents where Asian hacktivist groups are actively targeting nations like Israel, India, and even France, primarily due to their alignment with the U.S."

REFERENCE LINKS

- https://www.bleepingcomputer.com/news/security/microsoft-teams-phishing-attack-pushes-darkgate-malware/
- www.computingforgeeks.com/how-to-install-zabbix-on-rhel-centos-stream/#google_vignette
- https://thehackernews.com/2023/10/darkgate-malware-spreading-via.html
- https://thehackernews.com/2023/10/new-magecart-campaign-alters-404-error.html
- https://thehackernews.com/2023/10/cert-ua-reports-11-ukrainian-telecom.html
- https://thehackernews.com/2023/10/gaza-linked-cyber-threat-actor-targets.html
- https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-known-issue-causing-outlook-freezes-slow-starts/
- https://www.bleepingcomputer.com/news/security/over-40-000-admin-portal-accounts-use-admin-as-a-password/
- https://www.bleepingcomputer.com/news/security/over-10-000-cisco-devices-hacked-in-ios-xe-zero-day-attacks/#google_vignette
- https://www.bleepingcomputer.com/news/security/hackers-hijack-citrix-netscaler-login-pages-to-steal-credentials/
- https://www.bleepingcomputer.com/news/security/gnome-linux-systems-exposed-to-rce-attacks-via-file-downloads/
- https://www.bleepingcomputer.com/news/security/fbi-shares-avoslocker-ransomware-technical-details-defense-tips/

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