# Samples Details

# Samples in the First 30 Days

**I. 24d425448e4a09e1e1f8daf56a1d893791347d029a7ba32ed8c43e88a2d06439**

**SharpZeroLogon.exe**

**C4a97815d2167df4bdf9bfb8a9351f4ca9a175c3ef7c36993407c766b57c805b**

**SharpZeroLogon.exe**

**September 13, 2020**

EclecticIQ analysts observed the second hash listed above in EclecticIQ Intelligence Center in early Septermber 2020, just prior to its posting on VirusTotal or in Microsoft’s reporting. Microsoft reports initial attacks (2) confirmed by further reporting (3). The earliest observed malware post exploitation includes Cobalt Strike and web shell scripts. Both malwares are known for their use in establishing alternate command and control channels and expanding footholds post-initial compromise. EclecticIQ analysts note it is interesting that the earliest reports do not detail the malware associated with the initial compromise. It is unclear to what type of threat actors operating these attacks belong. Very similar malware is later used post-exploitation in the Kill-Chain of sample VII below.

Both files are posted by Microsoft in a Tweet on September 24, 2020 (<https://twitter.com/MsftSecIntel/status/1308941508809236480>). One of the same files is later present in a December 2020 report from FireEye regarding stolen tooling (<https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html>).

**II. a299912f3dc7cf0023aef8e4361abfc03e9a8c30
Mimikatz.exe (v 2.2.0)
September 16, 2020**

A custom version of Mimikatz credential stealer reported by a security researcher via social media (https://twitter.com/gentilkiwi/status/1306178689630076929). The version of Mimikatz contains further Windows scripting to help automate Zerologon exploitation; Netlogon brute-force scripts and PowerShell commands to reset an account password. In the same thread, the researcher credits “@SecuraBV” for details of the vulnerability.

# Samples at 30-90 Days

**III. b1c0d234dd058fa19a9f97fa6952192c9c4a24fd96cda2d235703fb402fe7afb
ff99453f07118c8738423bdeceeac96d.virus
October 29, 2020**

Remote access malware variant “Johnnie” is a simplified trojan that uses an automated plugin for Zerologon, created on October 29, 2020 and last sampled on February 24, 2022 (<https://www.virustotal.com/gui/file/b1c0d234dd058fa19a9f97fa6952192c9c4a24fd96cda2d235703fb402fe7afb>,<https://blog.talosintelligence.com/2019/01/threat-roundup-0111-0118.html>).

The file contents are not obfuscated. Upon execution it initiates WSASTARTUP to create a socket connection, and invokes wmiprvse.exe to leverage Windows Management Instrumentation (WMI). WMI is used with CONHOST to access a command prompt, where a password reset is then issued using “powershell.exe -c Reset-ComputerMachinePassword”.

# Samples at 90-180 Days

**IV. 3a8b7c1fe9bd9451c0a51e4122605efc98e7e4e13ed117139a13e4749e211ed0
zero.exe
November 25, 2020**

This file (https://www.virustotal.com/gui/file/3a8b7c1fe9bd9451c0a51e4122605efc98e7e4e13ed117139a13e4749e211ed0/details) uses a variety of discovery and fingerprinting to search for domain controllers. Once a target is selected it enumerates LDAP accounts, and finally launches “powershell.exe -c Reset-ComputerMachinePassword". The same file is implicated in a recent (2022) Cuba ransomware campaign report (https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis).

The same file is also present in a DFIR report detailing a 2021 Zerologon-based cyberattack (https://thedfirreport.com/2021/11/01/from-zero-to-domain-admin/). The file demonstrates how the circulation of exploitation modules can increase different cyberattacks.

# Samples at 180-360 Days

**V. F63E17FF2D3CFE75CF3BB9CF644A2A00E50AAFFE45C1ADF2DE02D5BD0AE35B0
cool.exe
November 15, 2021**

A version of Qbot and Cobalt Strike are the primary malware payloads paired with heavily automated Zerologon abuse functionality. This activity possibly extends back as early as November 2021 due to timestamps present within some malware
([https://thedfirreport.com/2022/02/21/qbot-and-Zerologon-lead-to-full-domain-compromise/](https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/)).
The added malware development includes further payload obfuscation through file encoding, and automated RDP connection.

**VI. B041432c77858519a79f500f35de48362686f987d8fdfe5c6ab7f632fc468942
SMSS.exe
February 02, 2022**

A crypto-mining bot, this Silent Miner variant provides command line access. The miner invokes VirtualProtect from KERNEL32 to segment and steal CPU resources for mining activities. (<https://www.virustotal.com/gui/file/b041432c77858519a79f500f35de48362686f987d8fdfe5c6ab7f632fc468942/detection>). All malware variants collect Monero and are still recently active in 2022 (<https://otx.alienvault.com/indicator/file/b041432c77858519a79f500f35de48362686f987d8fdfe5c6ab7f632fc468942>).

**VII. 36bc32becf287402bf0e9c918de22d886a74c501a33aa08dcb9be2f222fa6e24
zero.exe
November 6, 2020**

A sample created November 6, 2020, last submitted on June 28, 2021, and last analyzed on July 12, 2022 (<https://www.virustotal.com/gui/file/36bc32becf287402bf0e9c918de22d886a74c501a33aa08dcb9be2f222fa6e24/details>). This file matches a Florian Roth YARA rule detecting a Windows trojan. The file contains similar modules and functionality to the “\*.virus” variant described in sample (IV). The more recent version here is detected by more antivirus engines and does not contain the automated PowerShell script module that was configured in the earlier sample. The same sample is present in a CISA advisory for Darkside ransomware containing IOCs (<https://www.cisa.gov/uscert/ncas/alerts/aa21-131a>, <https://www.cisa.gov/uscert/sites/default/files/publications/AA20-131A.stix.xml>).
In the Darkside attack, operators used phishing for initial access, then deployed their own version of PSEXEC to exploit Zerologon using the “zero.exe” module.

# Samples After 360 Days

**VIII. 10ed27a6dad3793933262c0a0b4ec1837c7127cde872acf23e4c42a8ecfd9109
SharpZeroLogon.exe
December 8, 2020 and November 9 2021**

A file or tool that leverages Zerologon captured in VirusTotal and confirmed in further reporting (<https://www.virustotal.com/gui/file/10ed27a6dad3793933262c0a0b4ec1837c7127cde872acf23e4c42a8ecfd9109/details>, <https://www.picussecurity.com/resource/blog/techniques-tactics-procedures-utilized-by-fireeye-red-team-tools>, https://blog.qualys.com/vulnerabilities-threat-research/2021/02/01/unpacking-the-fireeye-breach-start-here-first).
The unsigned file is picked up by a YARA rule built by FireEye to detect one of their proprietary tools designed to test Zerologon (<https://github.com/Neo23x0/signature-base/search?q=HackTool_MSIL_SHARPZEROLOGON_1_>, <https://blog.qualys.com/vulnerabilities-threat-research/2021/02/01/unpacking-the-fireeye-breach-start-here-first>).
It is not encrypted and contains default strings “Program Data”, “Default Path”, “Set URL”, that would otherwise be configured with custom strings if the sample was captured during an actual attack. This configuration might be expected of an unmodified testing tool. The creation date of the file is spoofed to March 29, 2052. Three other tool variants contain similar spoofed creation dates, but contain differing registry keys and launch different processes (<https://www.virustotal.com/gui/file/c4a97815d2167df4bdf9bfb8a9351f4ca9a175c3ef7c36993407c766b57c805b/details>, <https://www.virustotal.com/gui/file/b9088bea916e1d2137805edeb0b6a549f876746999fbb1b4890fb66288a59f9d/detection>, <https://www.virustotal.com/gui/file/24d425448e4a09e1e1f8daf56a1d893791347d029a7ba32ed8c43e88a2d06439/detection>).

# Samples After 720 Days (2022 Activity)

**IX. 7421b0940e4f5dd5e3ac865f8093707357dd3e1168c6f167ec7cbd5b0727281c
python3-impacket\_0.10.0-1\_all.deb
May 6 2022**

The Linux file (<https://www.virustotal.com/gui/file/7421b0940e4f5dd5e3ac865f8093707357dd3e1168c6f167ec7cbd5b0727281c/detection>) uses python with Impacket to scan for Zerologon instances (<https://packages.debian.org/sid/python3-impacket>).

It is not known if these tools were used by security engineers or threat actors at the time of submission to VirusTotal, but the timing of timestamps is consistent with SolarWinds campaign activity prior to December 2020. It is possible that SolarWinds threat actors either used Zerologon to pivot deeper into compromised networks for tailored operations or provided the vulnerability testing tool they stole to another threat actor.

**X. afc2bdc76c05df76543417174e722531431265380a9227ebaa156d28b1bf5c7a
 Mimikatz.exe
 June 2, 2022**

Other Mimikatz password stealers such as (https://www.virustotal.com/gui/file/afc2bdc76c05df76543417174e722531431265380a9227ebaa156d28b1bf5c7a/details) are still present well into 2022. They contain the same PowerShell and Netlogon scripts recycled from earlier original TTPs. Scripts are launched from the same process trees in similar orders of execution. The malwares are detected by a Yara signature created to detect Zerologon activity (https://valhalla.nextron-systems.com/info/rule/SUSP\_PS1\_ResetComputerMachinePassword\_Nov21).

**XI. 5ad6233a0d3fb69262840a1e0b3fb1e113f2625a0629407ffd14ebec766938c5
b9087362e2cfb2535a3454af436b2a34.virus.
July 15, 2022**

This file and similar variants uploaded multiple times between May 9 and July 21 2022 include the same initial exploitation module for Zerologon and no additional payloads. This module allows threat actors to hide activity under the SVCHOST Windows process, invoke a command prompt and exploit Zerologon. Once privileges have been elevated, the malware invokes wmiprvse.exe where further scripts can be injected. <https://www.virustotal.com/gui/file/5ad6233a0d3fb69262840a1e0b3fb1e113f2625a0629407ffd14ebec766938c5/behavior/C2AE>. This type of generic injection under a common Windows service, packaged in a module designed to plugin to other malware via automated scripting, is evidence of further MaaS development that is much less tailored in terms of capabilities.

Appendix A.
Zerologon Provides an Exemplary Window into Common Vulnerability Attack Cycles

CVE-2020-1472 (Zerologon) was chosen to study for many reasons. Tenable rates it as the most significant vulnerability for all of 2020 (24). A later joint US-government alert rated the vulnerability as one of the most exploited that year (25). Qualys data further demonstrates Zerologon was one of five vulnerabilities responsible for 99% of vulnerable instances detected (26). CVE-2020-1472 provides both widespread and strategic access to varying target networks across the globe due to its implementation in many networks. The pandemic introduced a situation where EclecticIQ analysts expect higher-than normal attack activity due to many factors combined creating increased attack activity from many different threat actors.This evaluation is supported by large law enforcement datasets (27), and many cybersecurity reports detailing the increased risk due to increased attacks aimed at remote work-supporting systems (28, 29, 30, 31). The reported increased cyberattack activity coupled with a less than ideal patch rollout makes CVE-2020-1472 ideal for analysis because it very likely attracted a high degree of attention from many different threat actors.

## The Patch Rollout Very Likely Created a Situation For Increased Numbers of Systems to be Exposed and Not Fully Protected From All Related Cyberattacks

CVE-2020-1472 was disclosed on August 18, 2020 and a client-side patch was issued the same day. A further server-side patch also covering legacy deployments was issued six months later on February 9, 2021 to mitigate further issues. The CVE was initially rated 8.8 rather than the eventual 10.0 rating it later received due to further highlight of the server-side issue (1). Lower rating very likely created an environment for increased cyberattack due to mis prioritization. Other reporting supports this theory (32, 33, 34, 35).

# Appendix A Bibliography.

1. <https://www.tenable.com/blog/one-year-later-what-can-we-learn-from-Zerologon>
2. <https://us-cert.cisa.gov/ncas/alerts/aa21-209a>
3. <https://blog.qualys.com/vulnerabilities-threat-research/2021/02/01/unpacking-the-fireeye-breach-start-here-first>
4. <https://www.europol.europa.eu/media-press/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime>
5. <https://www.pwc.com/us/en/library/covid-19/making-remote-work-productive-secure.html>
6. <https://www.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe>
7. <https://link.springer.com/article/10.1057/s41284-021-00286-2>
8. <https://threatresearch.ext.hp.com/hp-wolf-security-blurred-lines-blindspots-report-risky-remote-working/>
9. <https://www.darkreading.com/vulnerabilities-threats/one-year-later-a-look-back-at-zerologon>
10. <https://us-cert.cisa.gov/ncas/current-activity/2020/09/14/exploit-netlogon-remote-protocol-vulnerability-cve-2020-1472>
11. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472>
12. <https://support.microsoft.com/en-us/topic/how-to-manage-the-changes-in-netlogon-secure-channel-connections-associated-with-cve-2020-1472-f7e8cc17-0309-1d6a-304e-5ba73cd1a11e>