TDX ARENA

Certification Report

Kevin Martinho
Final Assessment Report Submission

One of Us: [Critical Security Incident - System Compromise and Malware Infrastructure]

December 6, 2025

Overview

During this investigation, it was discovered that Bruce's workstation has been seriously compromised by an attacker who is actively using it right now. The attacker has set up multiple ways to keep access to the system, including remote desktop software (XRDP), fake DNS settings, and has stored 272 malicious files on the computer. Active connections were also found to external servers controlled by the attacker, which means they are currently connected to Bruce's system and communicating with it in real-time. Review of the XRDP configuration file (/etc/xrdp/xrdp.ini) revealed that remote access restrictions were not properly configured, allowing the attacker to establish unrestricted remote desktop sessions without authentication controls. A statistical analysis script was used to establish a baseline of normal file characteristics across all 272 files, which identified file0.exe and file176.exe as significant anomalies based on byte repetition patterns, indicating PE overlay injection with encrypted malware payloads.

Technical Findings

A custom bash script was developed to perform anomaly detection by analyzing byte repetition patterns across all 272 files in the suspicious directory. The script established a baseline average of 34% byte repetition (normal range), with a standard deviation of 2%, setting an anomaly threshold at 38%. File0.exe and file176.exe were flagged as critical anomalies with 45-46% byte repetition—over 6 standard deviations above the mean—indicating they are not normal files but rather contain obfuscated or encrypted payloads. These findings were corroborated by VirusTotal detections confirming overlay injection techniques. Additionally, someone modified Bruce's system's hosts file (a critical system file) to redirect antivirus tools to fake websites that the attacker controls. This fake antivirus interface tells Bruce everything

is fine when it's actually not. When checking what network connections Bruce's computer was making, active connections were found to the attacker's servers - meaning they have a live session on Bruce's computer right now, and they're actively using remote desktop to control it. The XRDP service was also configured to auto-start at boot, meaning even after a system restart, the attacker would regain access without needing to reinstall the backdoor.

Recommendations

Bruce needs to immediately disconnect his computer from the internet and turn it off to protect any evidence. He should then report this to law enforcement and provide them with the attacker's IP addresses, the malware file information, and screenshots of the connections. A forensics professional needs to examine Bruce's hard drive to figure out exactly what the attacker accessed and whether they got to other computers on his network. Going forward, Bruce should implement automated malware detection scripts like the one used in this investigation to establish baselines and identify anomalies in file systems, disable or uninstall XRDP entirely unless necessary, and if remote access tools are needed, configure them with strong authentication, IP whitelisting, and access logging enabled. Bruce should also check all other computers connected to his network to make sure they haven't been attacked the same way, implement network segmentation to isolate critical systems, and upgrade his security tools to catch this type of attack in the future.

Findings and Analysis

Present the findings relevant to the investigation in a structured and detailed manner. For each finding, explain its cybersecurity context and its significance to the investigation.

Note: Select up to 5 relevant findings from the list provided in *Appendix A* at the end of this document.

Example:

Finding	Finding Details	Description
3389	93.243.107.34 172.12.0.28 172.18.0.29	Open port that was discovered using netstat command. Multiple streaming connections to XRDP_disconnet_display_10, xrdp_display_10 and @/tmp/.X11 Etc/hosts file reveals DNS poisoning of clamav-ui (a legit tool) and redirection of "workstation" to the attackers IP.

This port was discovered by inspecting the active network connections and associated executables on the target machine. The port appeared to be related to an executable…

Finding	Finding Details	Description
Malicious File	File0.exe – 35% File176.exe – 46%	Both Files are found to deviate from baseline byte repetition of other 270 files in 'suspicious-files.' Closer look revealed File176.exe to have padded UTF-16 null bytes.

This file appears to be a trojan installed by an attacker.

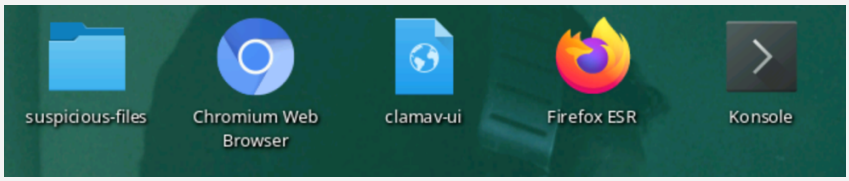
Methodology

Tools and Technologies Used

- **ps aux:** Running processes, timestamps, PID, CPU usage and file locations reveal more information about intrusion. This provided a good starting point on target machine.
- **Netstat**: Netstat is a command-line tool used to display network connections and network protocol statistics. I used netstat to review the open ports on the target machine.
- **/etc/hosts**: Discovered there were hosts
- **Bash**: Bash script established a baseline of the 272 files, seeks deviation, high bye repetition to indicate obfuscation and singled out file0 and file176.
- **VirusTotal**: Software that searches database for known signatures. This allowed me to find file0.exe was malicious and explore other files for more information about this attack.

Investigation Process

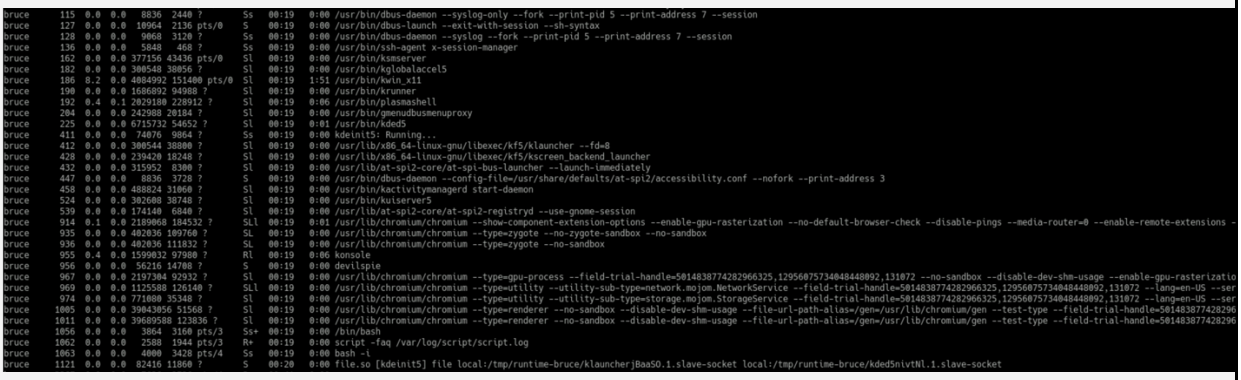
At first glance, there were some files listed on the desktop such as clamav-ui, Chromium Web Browser, suspicious-files, Firefox ESR and Konsole. This computer was owned by user, "bruce."



1. I ran the "*ps aux*" command to investigate what processes are being run. The first thing I noticed was that XRDP was restarted with elevated privileges as root and running a bash shell in 00:18 seconds. Further down the list is a script.log that I was not unable to access. This suggests a backdoor was created using XRDP and scripts/commands are being logged in the script.log.

```
bruce@workstation:/usr/lib/xorg$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0   2384   764 pts/0    Ss   00:18   0:00 /bin/sh -c sudo /etc/init.d/xrdp restart && bash
root          25  0.0  0.0  10600  3396 pts/0    S    00:18   0:00 /usr/sbin/xrdp-sesman
xrdp          30  0.0  0.0   7244  2172 pts/0    S    00:18   0:00 /usr/sbin/xrdp
root          50  0.0  0.0   3732  2908 pts/0    S+   00:18   0:00 bash
root          55  0.0  0.0   2588  1852 pts/0    S+   00:18   0:00 script -faq /var/log/script/script.log
root          56  0.0  0.0   3996  3256 pts/1    Ss+  00:18   0:00 bash -i
```

Increased CPU usage is seen after the daemon is running as XRDP and actively setting up a graphical user interface as a KDE service. A full desktop environment was established as well as a server (kuiserver). Multiple processes can be seen running a Chromium browser, terminal emulator and automating windows management (devilspie).



2. The "*netstat*" command shows established connections with multiple workstations and their ports. These connections are streaming and running.

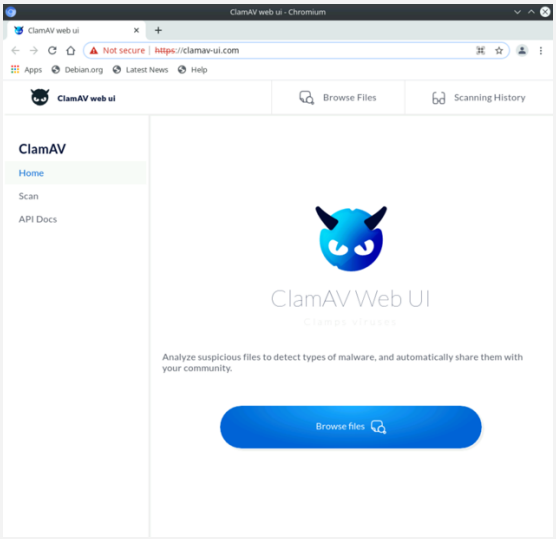
```
bruce@workstation:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 workstation:54422       bl-in-f94.1e100.n:https ESTABLISHED
tcp        0      0 workstation:49792       bk-in-f94.1e100.n:https ESTABLISHED
tcp        0      0 workstation:57644       bk-in-f84.1e100.n:https ESTABLISHED
tcp        0      0 workstation:38124       ww-in-f94.1e100.n:https ESTABLISHED
tcp        0      0 workstation:32876       123.35.104.34.bc.g:http ESTABLISHED
tcp        0      0 workstation:53466       pd-in-f95.1e100.n:https ESTABLISHED
tcp6       0      0 workstation:3389        ip-172-17-0-71.ec:60104 ESTABLISHED
```

```
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    136719557 /var/run/xrdp/sockdir/xrdp_disconnect_display_10
unix  3      [ ]         SEQPACKET  CONNECTED     136702551 @03049
unix  3      [ ]         SEQPACKET  CONNECTED     136702549 @03048
unix  3      [ ]         SEQPACKET  CONNECTED     136638949
unix  3      [ ]         STREAM     CONNECTED     136609674
unix  3      [ ]         STREAM     CONNECTED     136680650 @/tmp/dbus-t5LfFYc1TW
unix  3      [ ]         STREAM     CONNECTED     136616515
unix  3      [ ]         STREAM     CONNECTED     136611655
unix  3      [ ]         STREAM     CONNECTED     136715614 @/tmp/.X11-unix/X10
unix  3      [ ]         STREAM     CONNECTED     136694114 @/tmp/dbus-OObDotTG4t
unix  3      [ ]         STREAM     CONNECTED     136603647 @/tmp/.X11-unix/X10
unix  3      [ ]         STREAM     CONNECTED     136638946
unix  3      [ ]         STREAM     CONNECTED     136704171 /var/run/xrdp/sockdir/xrdp_display_10
unix  3      [ ]         STREAM     CONNECTED     136632287 @/tmp/dbus-t5LfFYc1TW
unix  3      [ ]         STREAM     CONNECTED     136733383 @/tmp/.X11-unix/X10
unix  3      [ ]         STREAM     CONNECTED     136694196 @/tmp/dbus-OObDotTG4t
unix  3      [ ]         STREAM     CONNECTED     136736773 @/tmp/.ICE-unix/162
unix  3      [ ]         STREAM     CONNECTED     136715617 @/tmp/.X11-unix/X10
unix  3      [ ]         STREAM     CONNECTED     136638947
unix  3      [ ]         STREAM     CONNECTED     136641379
unix  3      [ ]         STREAM     CONNECTED     136703154
unix  3      [ ]         STREAM     CONNECTED     136701176 @/tmp/.X11-unix/X10
unix  3      [ ]         STREAM     CONNECTED     136628218 @/tmp/dbus-OObDotTG4t
unix  3      [ ]         STREAM     CONNECTED     136679885
unix  3      [ ]         STREAM     CONNECTED     136698509
unix  3      [ ]         STREAM     CONNECTED     136659438 @/tmp/.X11-unix/X10
unix  3      [ ]         STREAM     CONNECTED     136641241 @/tmp/dbus-t5LfFYc1TW
unix  3      [ ]         STREAM     CONNECTED     136719594
unix  3      [ ]         SEQPACKET  CONNECTED     136638948
unix  3      [ ]         STREAM     CONNECTED     136737795 @/tmp/.X11-unix/X10
unix  3      [ ]         STREAM     CONNECTED     136588156
unix  3      [ ]         STREAM     CONNECTED     136719755 @/tmp/dbus-OObDotTG4t
unix  3      [ ]         STREAM     CONNECTED     136659478 @/tmp/dbus-t5LfFYc1TW
unix  3      [ ]         STREAM     CONNECTED     136635307
unix  3      [ ]         STREAM     CONNECTED     136678681
unix  3      [ ]         STREAM     CONNECTED     136674831
unix  3      [ ]         STREAM     CONNECTED     136659419 @/tmp/.X11-unix/X10
unix  3      [ ]         STREAM     CONNECTED     136628212
unix  3      [ ]         STREAM     CONNECTED     136653697 /tmp/runtime-bruce/plasmashellvnfVPy.1.slave-socket
unix  3      [ ]         STREAM     CONNECTED     136627714 @/tmp/dbus-t5LfFYc1TW
unix  3      [ ]         STREAM     CONNECTED     136662213
unix  3      [ ]         STREAM     CONNECTED     136734821
unix  3      [ ]         STREAM     CONNECTED     136711451 @/tmp/.X11-unix/X10
unix  3      [ ]         STREAM     CONNECTED     136664870
unix  3      [ ]         STREAM     CONNECTED     136705249
unix  3      [ ]         STREAM     CONNECTED     136682845
unix  3      [ ]         STREAM     CONNECTED     136588155
unix  3      [ ]         STREAM     CONNECTED     136611662
unix  3      [ ]         STREAM     CONNECTED     136665287 @/tmp/.ICE-unix/162
unix  3      [ ]         STREAM     CONNECTED     136712466
unix  3      [ ]         STREAM     CONNECTED     136614450
unix  3      [ ]         STREAM     CONNECTED     136734822
unix  3      [ ]         STREAM     CONNECTED     136614505 @/tmp/dbus-t5LfFYc1TW
unix  3      [ ]         STREAM     CONNECTED     136635305
```

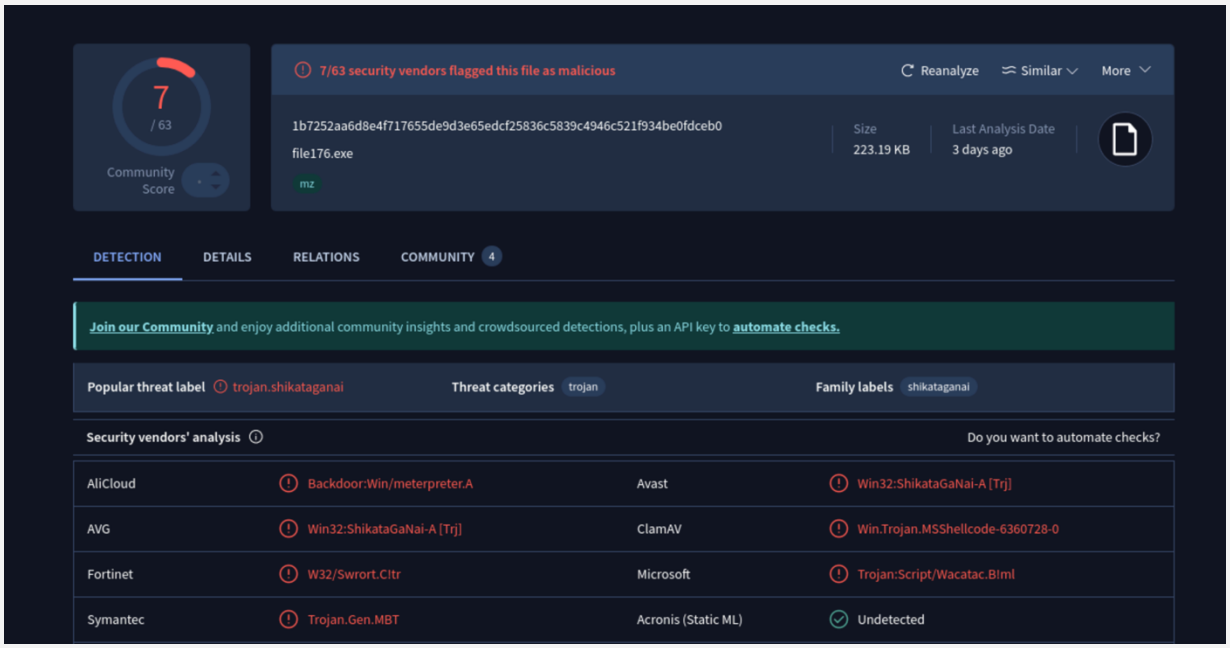
3. Check /etc/hosts file. Further review of the hosts file revealed that it was tampered with. There are multiple workstations with various ports that connect to the attacker machine. Attacker is rotating the ip addresses as they previously showed 172.17.0.28 and 172.17.0.29. The name "workstation" has been hijacked and will defer to the attacker ip address and port number. The fake website "clamav-ui" points to the attacker ip address.

```
bruce@workstation:/etc$ cat hosts
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.17.0.65     clamav-ui.com clamav-ui.com ecs-one-of-us-ed8800e9-a3d7-43b6-8728-87b342b075df-8-one-of-us-nodejs-bcf6c1a8a9efb8f18f0
1
172.17.0.70     workstation
```

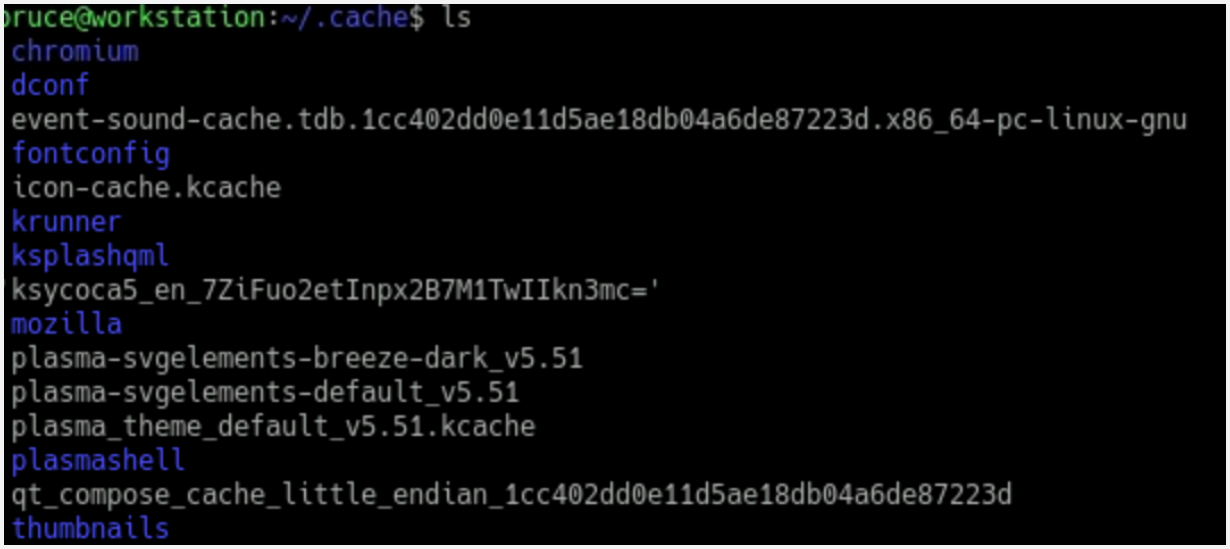
3. Chromiun browser shows the url “http.clamav-ui.com” and the interface resembles ClamAv an antivirus software. This is a fake website.



4. VirusTotal database scoured through the 272 suspicious-files folder. There were some clues derived from using MD5 hashes of those files.



5. Reviewing the ~/.cache files shows there is evidence of compromised activity with malicious code designed to steal credentials, startup before login, compromised browsers and obfuscation.



Recommendations

1. Isolate the system immediately and disconnect from the internet. Power off the system.
2. Contact the appropriate authorities and preserve evidence.
3. Scan other workstations on the same network as “Bruce’s”
4. Review configurations of the network, firewalls, blacklisting, whitelisting, ACL.
5. Enable DNSSEC extensions to prevent spoofing, configure filtering to block malicious domains and data exfiltration.
6. Look into DNS threat intelligence feeds for monitoring, alerts for DNS tunneling and queries.
7. Integrate integrity monitoring of files and make /etc/hosts file and the /etc/xrdp.ini immutable on ALL systems. Consider removing XRDP for all systems except those that require administration access.
8. Update and add the malicious file signature to the AV.
9. Train employees to identify and avoid accessing website with “Not Secure” and “http” certificate warnings.

File-related Findings	
Malicious File	~/Desktop/suspicious-files/file0.exe & file176.exe
Hash	928db29e105495fb78a976999ed5a98d – file0.exe f48a8687e91fd9ef98cd1b7aaeeb2a4c – file176.exe
File Attribute	.exe, file.so, f.txt, microstub
Network-related Findings	
IP Address	172.17.0.28, 172.17.0.29, 172.17.0.65, 172.17.0.70, 172.17.0.71
Port	3389, 54422, 49792, 57644, 38124, 32876, 53466
URL/API	http://clamav-ui.com
Packet Attributes	
Endpoint-related Findings	
Host	clamav-ui.com clamav-ui.com ecs-one-of-us-ed8800e9-a3d7-43b6-8728-87b342b075df-8-one-of-us-nodejs-948cdf81cbffb28f3f0
Registry Key	Relevant registry keys
User	bruce
Process	25, 30, 186
Adversary-related Findings	
Attack	Trojan, Backdoor, meterpreter, shellcode
Technique	Overlay Injection T1027 - Obfuscation Files and Software Packing T1071 – Application Layer Protocol DNS Poisoning T1557.002 – ARP Cache Poisoning Persistence T1547.013 – Boot/Login Initialization Scripts

	T1547.015 – Login Items T1112 – Modify System Configuration Cache T1555 – Credentials from Password Stores T1539 – Steal Web Session Cookie