Caylan Barnes, Bryan Mileski

Dr. Gonzalo De La Torre Parra

Digital Forensics 3345

10 December 2025

Digital Forensics Project Report

Throughout this semester, we have been tasked with analyzing a network system to discover and identify an attack within the system. We delegated the roles as follows, Lead Investigator appointed to Mileski, Evidence Analysts were assigned to both Mileski and Barnes, and lastly, the Documentation Lead was assigned to Barnes.

We began by preparing and setting up our systems. This included a Kali Linux Virtual Machine, where we imported the CTU-13 PCAP dataset and conducted a forensic review. Zeek for botnet network traffic analysis so we could uncover the attackers' IP addresses and infected machines, C2 channels, evidence, malware propagation, and signs of spam or data exfiltration. Wireshark to extract files from the PCAP file and save suspicious intact files to calculate their hash. Lastly, we used Virus Total to identify any malicious files by searching for their hashes. The dataset we used for this analysis was an evidence file, botnet-capture-20110815-fast-flux.pcap, and the hashes MD5, SHA-1, and SHA-256.

By analyzing the PCAP file, we uncovered some suspicious activity within the network system. We found that there were 88,049 connections with source IP address 147.32.84.165. With destination IP addresses, we found 64,162 connections with IP address 184.173.217.40, and 4,820 connections with 147.32.80.9. The top protocols present were 80,232 connections with these unidentified protocols: DNS, HTTPS, SSL, SMTP, DCE_RPC, and RDP. We uncovered a custom C2 channel within our network, having 676 connections to IP address 212.117.171.138,

using an unusual port 65500 while maintaining long-lived TCP sessions. We deduced that this was likely an encrypted or proprietary protocol, since there were no associated service banners. Furthermore, we noticed a large amount of SMTP traffic, having 13,204 SMTP connections to port 25 and 140 secure SMTP connections to port 587. We concluded that the infected host was likely being used as a spam relay or email-distribution bot, contributing to malicious campaigns or data exfiltration. The abnormal volume of email traffic indicated that the host was compromised as part of the botnet operations. We found internal connections using Windows-sharing protocols, which are prevalent in worm propagation. This evidence suggests the bot attempted a local network infection to expand the botnet footprint, scanning or exploiting vulnerable Windows hosts. The SMB/NTLM activity indicated the possible lateral movement within our network. There were also DNS abnormalities and fast-flux indicators within our system, with 4,821 outbound DNS queries and 4,891 DNS service events. The queries were heavily directed at IP address 147.23.80.9, a DNS server. This pattern strongly matches Domain Generation Algorithm (DGA) behavior, used by botnets like Conficker to evade takedown. We concluded that the massive DNS traffic and rapidly changing domains revealed the behavior that was used to conceal the botnet infrastructure. We also found evidence that was encrypted over HTTPS, with 64,162 connections to 184.173.217.40 on port 443, which is far beyond normal web-browsing activity. The C2 encryption allowed the malware to hide inside the TLS traffic. We concluded that the malware likely used HTTPS as its main encrypted communication channel for sending system data and receiving commands. The bot relied on HTTPS for stealthy, encrypted command-and-control communication.

We noticed that, in all, IP address 147.32.84.165 had the most documented connections. Each connection was initiated in roughly five-second intervals, which indicated that this was a

bot automation rather than a human browsing. The connection state field is an “RSTR”, meaning the responder resets the connection, rather than terminating the session as normal. IP address 209.173.182.133 was communicating on port 3389, standard for Remote Desktop Protocol. We reconstructed the attack methodology, which suggested the attack began on Monday, August 15, 2011. We further investigated and found on that date at 10:19 am that the IP address 147.32.84.165 sends a GET request to IP address 94.63.149.152 for a suspicious URI called /rus.php. At 10:21 am, IP address 91.220.0.52 sends a POST request of more than 200,000 bytes to the suspected infected host 147.32.84.165, a total of five times. At 2:49 pm, IP address 147.32.84.165 then sends a GET request to IP address 60.190.223.75 for a suspicious download called /p/out/kp.exe. AT 8:43 pm, IP address 209.173.182.123 initiates connections with 147.32.84.165 every five seconds through an RDP protocol. With the evidence we gathered, we concluded that this is indeed how the host became infected, and bots were able to infiltrate the system.

IP address 147.32.84.165 initiated many connections that occurred at steady intervals, a characteristic of bot malware, and is most likely a C2C beaconing. IP address 209.173.182.133 tried to connect to the already compromised IP address 147.32.84.165 at repeated intervals through RDP, with all connections being reset instead of terminated as normal. We concluded that this could be a multi-stage attack. The attacker compromised IP address 147.32.84.165 which propagated malware activity and C2C beaconing activity to maintain a persistent channel to the C2 server, allowing the attacker to get a foothold in the network. For the next stage, the attacker, IP address 209.173.182.133, tried to get full control of the network through RDP by connecting to IP address 147.32.84.165. Through the RDP, the attacker can escalate their

privileges and better explore the network, look for valuable files and sensitive information, configure backdoors, and disable security.