In this intrusion, dated May 2023, we observed Truebot being used to deploy Cobalt Strike and FlawedGrace (aka GraceWire & BARBWIRE) resulting in the exfiltration of data and the deployment of the MBR Killer wiper. The threat actors deployed the wiper within 29 hours of initial access.

Case Summary

In this case, Truebot was delivered through a Traffic Distribution System (TDS) reported by Proofpoint as “404 TDS”. This campaign, observed in May 2023, leveraged email for the initial delivery mechanism. After clicking-through the link in an email, the victim would be redirected through a series of URLs before being presented a file download at the final landing page.

The file download was a Truebot executable, which appeared as a fake Adobe Acrobat document. After executing the file, Truebot copied and renamed itself. Minutes later, Truebot loaded FlawedGrace onto the host. While loading this malware, it used a series of modifications to the registry and Print Spooler service to both escalate privileges and establish persistence. From there, FlawedGrace’s execution routine involved storing as well as extracting, encoded and encrypted payloads in registry; the creation of temporary scheduled tasks and the injection of the final payload into msiexec.exe and svchost.exe.

After this execution, the threat actors proceeded to disable Windows Defender Real-Time monitoring and added exclusions for executable files on the host. We later observed FlawedGrace creating a temporary user within the local Administrators and Remote Desktop Users groups. With this user, a tunneled RDP connection was attempted from FlawedGrace’s C2 servers. Seemingly without success, the threat actors removed the user after 15 minutes before repeating the procedure a second time. After the second failed attempt, the threat actors removed the user and did not attempt further RDP communications. The FlawedGrace process then performed discovery surrounding the domain administrators and domain controllers.

Approximately two hours after the initial execution, Truebot loaded Cobalt Strike into memory and then went dormant for the next two hours. This ended the use of Truebot for the rest of the intrusion, with FlawedGrace and Cobalt Strike being leveraged for the rest of the threat actors activity. Now, four hours into the intrusion the threat actors, through the Cobalt Strike beacon, started another round of discovery commands using net, nltest, tasklist and AdFind.exe.

After having accessed LSASS memory on the beachhead host, the threat actors leveraged a local administrator hash to perform pass-the-hash lateral movement through the environment. The threat actors used Impacket’s atexec to execute discovery commands on remote hosts. These discovery commands included the PowerShell, cmdlet Get-MpComputerStatus, and quser. After these discovery

commands, the threat actors used Cobalt Strike's jump psexec module to further move between hosts. Following each lateral movement action, Cobalt Strike loaded FlawedGrace in memory on all hosts accessed by the adversary.

Around five hours post initial access, the threat actors went silent. FlawedGrace and Cobalt Strike went dormant on all hosts except the beachhead system. Seventeen hours later, the threat actors returned to the network and issued enumeration commands to discover network shares. Around that time, we observed signs of data exfiltration from the environment.

Roughly four hours after the exfiltration began, merely 29 hours into the intrusion, the threat actors deployed the MBR Killer wiper on all hosts where FlawedGrace had been running, including a file server. This executable overwrote the MBR (Master Boot Record) and triggered a reboot, rendering the hosts unusable. Numerous systems were left at the boot screen, inoperable.

Following these actions, the threat actors lost all footholds to the network. While data has been exfiltrated, no responsibility has been claimed and no extortion notes were found.

Attribution

Truebot (a.k.a. Silence.Downloader) has been attributed to the Silence group which have had long standing interactions with financially motivated criminal group TA505 (spammer/distribution). The FlawedGrace malware has been reportedly associated, but not exclusive, to TA505, and has commonly been distributed by Truebot.

Most recently, an activity group reported by Microsoft as Lace Tempest was observed running a Cl0p extortion operation. According to Microsoft "Lace Tempest (DEV-0950) is a Clop ransomware affiliate that has been observed using GoAnywhere exploits and Raspberry Robin infection hand-offs in past ransomware campaigns."

"Lace Tempest operates in two modes. One mode where they deploy Cl0p enterprise wide and the other where they do mass exploitation against file transfer servers – and steal data (and possibly deploy mbrkiller). Both sets of victims show up on Cl0p leak site. Even if the ransom payload wasn't deployed."

– Christopher Glyer, Principal Security Researcher with Microsoft Threat Intelligence

The MBR Killer binary in this case was attributed to the Lace Tempest activity group per Microsoft. Microsoft also recently attributed the MOVEit Transfer 0-day (CVE-2023-34362) exploitation to Lace Tempest.

According to Mandiant, in January 2023 FIN11 was observed deploying TRUECORE (a version of Truebot) and BARBWIRE (FlawedGrace) after exploiting a SolarWinds Serv-U server (CVE-2021-35211). During this time, BARBWIRE C2 was communicating with 5.188.86[.]18:443, which we observed in this case. In April, Mandiant again observed BARBWIRE C2 communicating to 5.188.86[.]18:443 as well as 92.118.36[.]199:443, which was also observed during this case. During this time period, Mandiant also noted that shellcode payloads were staged on a TRUECORE C2 server, which pointed to 5.188.206[.]78, the Cobalt Strike server in this case. Mandiant also confirmed that they've observed FIN11 using MBR Killer as early as 2019. According to Mandiant, FIN11 has used BARBWIRE since at least 2018, and they believe that the backdoor is exclusive to the threat group. Mandiant also recently attributed the MOVEit Transfer 0-day (CVE-2023-34362) exploitation to FIN11.

Due to the overlap of TTPs, we are attributing this intrusion with high confidence to Lace Tempest and FIN11 with possible TA505 overlaps.

Services

We offer multiple services including a Threat Feed service which tracks Command and Control frameworks such as Cobalt Strike, Metasploit, Empire, PoshC2, etc. More information on this service can be found here.

Our All Intel service includes private mini reports, exploit events, long term infrastructure tracking, clustering, C2 configs, and other curated intel, including non-public case data.

If you are interested in hearing more about our services, or would like to talk about a free trial, please reach out using the Contact Us page. We look forward to hearing from you.