Case Summary

In early November 2022, the intrusion began with the delivery of an HTML file. We assess with high confidence that the delivery was via email, as reported in other public reports. This HTML file was using a technique known as HTML smuggling. This is one of the techniques threat actors have pivoted to since macro control defaults were updated by Microsoft. Just a month prior, this threat actor was observed using Excel macros in an extremely similar campaign.

Upon the user opening the HTML file, a fake Adobe page was presented and a ZIP file was downloaded. The Adobe lure includes a password for the ZIP as a way to protect the malicious contents from automated analysis. Inside the ZIP was an ISO file. Inside the ISO was the malware payload. The only visible file to the user was a LNK file masquerading as a document.

When the user clicked the LNK file, a series of commands were then executed. These included copying rundll32 and a malicious DLL from within the ISO to the host, before executing the malware. After loading the malicious DLL, a connection was made to IcedID command and control servers. The user meanwhile was served a legitimate image of a finance document.

When the malicious DLL was executed, persistence was also established via a scheduled task on the beachhead host. This task was set to run the IcedID malware every hour on the host. Initial discovery commands were ran seconds after reaching out to the command and control server. These commands have been seen in previous reports involving IcedID, including standard utilities like net, ipconfig, systeminfo, and nltest.

Around three hours after execution of the initial IcedID malware, a cmd process was spawned from IcedID. This new process began beaconing to a Cobalt Strike server. This Cobalt Strike server was previously observed in a prior Nokoyawa report. This process was then observed accessing LSASS, likely to access credentials. A quick check of domain admins using net was also observed.

Hands-on activity then paused for around three hours before the threat actor returned. Using the Cobalt Strike beacon, the threat actor looked up specific domain administrators using the net utility. Using one of those accounts, the threat actor initiated a RDP session to move laterally to a domain controller. Using this session, the threat actor copied over a Cobalt Strike beacon to the domain controller and executed it.

After that, the threat actor continued discovery actions by executing a batch file on the domain controller, which ran the usual battery of Active Directory discovery commands using AdFind. Upon completion, the results of the discovery commands were archived using 7-Zip. This was followed by the threat actor running a second batch file, which iterated through the network performing a nslookup for each host in the environment.

About five hours later, the threat actor returned to the domain controller and executed an encoded PowerShell command which was SessionGopher. SessionGopher is a tool that finds and decrypts saved session information for remote access tools. The threat actor then logged into additional hosts over RDP, including a backup server and a server with file shares. On the backup server, the threat actor opened the backup console. While on the file share, they used notepad to review a file on the host.

The threat actor returned to the domain controller and utilized netscan to perform a network scan. After the scan, both PsExec and WMIC were used to move files across systems in the network. Key files copied included k.exe and p.bat. These two files were the ransomware binary and a batch script that would be used to execute the ransomware.

Five minutes after transferring the files to hosts in the domain, the Nokoyawa ransomware binary was executed on a domain controller. At the same time, PsExec was used to execute the p.bat file starting the ransomware binary on the other hosts in the domain. The time to ransomware (TTR) was just over 12 hours from the initial infection.

Attribution

In this case we see two different threat actors; the distributor and the hands on keyboard actor. Proofpoint tracks this distributor as TA551. The hands on keyboard actor is tracked by Microsoft as Storm-0390 which is a “pen test” team managed by Periwinkle Tempest (formerly tracked as Storm-0193 and DEV-0193).

The ransomware affiliate is seen RDPing into the environment from server name WIN-5J00ETD85P5. This server name matches the one used by a threat actor from a prior Nokoyawa case. We can see from internet scanning tools, this hostname is currently active on 78.128.113[.]154 hosted on AS209160 Miti2000 at 4vendeta.com in Bulgaria.

Services

We offer multiple services including a Threat Feed service which tracks Command and Control frameworks such as Cobalt Strike, Metasploit, Empire, Havoc, 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.

We’ll be launching a private ruleset soon, if you’d like to get in at a discounted rate for the beta, please Contact Us.

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.

Analysts

Analysis and reporting completed by @v3t0_, @AkuMehDFIR, &
@RoxpinTeddy