A Tale of PivNoxy and Chinoxy Puppeteer

August 22, 2022

Recently, a simple and short email with a suspicious RTF attachment that had been sent to a telecommunications agency in South Asia caught the attention of FortiGuard Labs. The email was disguised as having come from a Pakistan government division and delivered the PivNoxy malware.

Affected Platforms: Windows
Impacted Parties: Windows users
Impact: Controls victim's machine and collects sensitive information
Severity Level: Medium

This blog describes how the attack works, suggests who the threat actor behind the operation might be, and details the techniques used by the attacker.

Attack Overview

The attack started with a simple email that included a bare document as an attachment:

Figure 1. Spearphishing email used in the attack

The attached doc file is in RTF format. It was generated using a tool called Royal Road, a phishing “weaponizer” believed to be used by several Asia-based APT threat actors. Also referred to as 8.t RTF exploit builder, Royal Road allows APT groups to create RTF files with embedded objects that can exploit vulnerabilities in Microsoft Word to infect targets. Some of the known vulnerabilities that Royal Road supports include:

- CVE-2017-11882 (Microsoft Office Memory Corruption Vulnerability)
- CVE-2018-0802 (Microsoft Office Memory Corruption Vulnerability)
- CVE-2018-0798 (Microsoft Office Memory Corruption Vulnerability)

Opening the email attachment, “Please help to CHECK.doc,” opens a decoy Word document. And at the same time, it exploits CVE-2018-0798 in the background. CVE-2018-0798 is a Remote Code Execution (RCE) vulnerability in Microsoft’s Equation Editor (EQNEDT32). Microsoft released a fix for it on January 9, 2018. The fact that attackers are still targeting this vulnerability highlights that not all organizations deploy critical patches or upgrade to the latest software. The truth is that older vulnerabilities are still commonly and successfully being exploited.

Figure 2. Decoy Word file used in the attack. Note that gibberish displayed in the document may be a result of the language not being supported by our test machine.

Once executed, the malicious document drops three files:

- *C:\\ProgramData\Cannon\Cannondriver.exe*
- *C:\\ProgramData\Cannon\LBTServ.dll*
- *C:\\ProgramData\Cannon\Microsoft.BT*

Despite the deceptive file name, the Cannondriver.exe file is a legitimate Logitech file, LBTWizGi.exe, with the description, “Logitech Bluetooth Wizard Host Process.” The Cannondriver.exe is even digitally signed by a certificate issued to Logitech.

Figure 3. Legitimate version of Cannondriver.exe

On the other hand, the *LBTServ.dll* file is not digitally signed. This is where it gets interesting. “*Cannondriver.exe”* is vulnerable to a DLL Search Order Hijacking attack that *LBTServ.dll* takes advantage of. Take note that the *“LBTServ.dll”* sample used in this attack has a compilation time of Sun July 18 02:04:24 2021 GMT. This means that this group created this variant well before they needed to use it. It suggests they were either ready to attack their target almost a year before or had started stockpiling an arsenal of malware ready to go at a moment’s notice. Recent Chinoxy samples that stayed under the radar, but were uncovered during our investigation, have similar compile times.

Figure 4. DLL Search Order Hijacking inside Cannondriver.exe

The figure above is part of the code found in *Cannondriver.exe.* Basically, it calls the export named *LGBT_Launch,* which is found in *LBTServ.dll.*

Figure 5. Inside LBTServ.dll

After *Cannondriver.exe* loads the fake *LBTServ.dll* and calls the *LGBT_Launch* function, the malicious function loads the other dropped file, *Microsoft.BT*, into memory and proceeds to decrypt it. The attack chain is similar to that used by the Chinoxy backdoor, which also uses Cannondriver.exe to load a malicious LBTServ.dll to deliver its payload.

However, this current variant sent to the telecommunication agency in South Asia delivers the final payload a bit differently than its predecessors. Instead of LBTServ.dll containing the final payload, it loads a shellcode from a separate file and injects itself into *svchost.exe.* It then contacts *instructor[.]giize[.]com,* a dynamic DNS redirecting the connection to the attacker’s IP where the payload is hosted. Unfortunately, a remote file was not available at the time of this investigation. Luckily, a tweet by nao_sec identified PoisonIvy malware as the payload.

Figure 6. Tweet by nao_sec on May 12, 2022

PoisonIvy is a Remote Access Trojan (RAT) that has been around for over a decade. Also known as Pivy, the RAT is distributed in underground forums and allows an attacker to take control of a compromised machine and perform reconnaissance activities through its GUI.

FortiGuard Labs previously released a blog series detailing how PoisonIvy works:

The PoisonIvy RAT variant covered in those blogs performs lateral movement. As such, a single infection by PoisonIvy can lead to information being lifted from a wide range of machines in the affected organization.

The Quest to Reveal the Attacker’s Identify

Although PoisonIvy is known to have been used in targeted attacks, it’s not an easy task to identify the attacker behind the operation targeting the telecommunication organization in South Asia. This is due to the number of reported threat actors that use the RAT and its wide availability.

Our curiosity about the attacker led to another LBTServ.dll (SHA2: 719f25e1fea12c8dc573e7161458ce7a5b6683dee3a49bb21a3ec838d0b35dd3), that was submitted to VirusTotal from France in January 2022. This file is dropped by a file with SHA2: cdf417e67b0aaf798ac7c0f9ccb8b5b21f09b408ee6748beea5e03e76902e7fe.

Our analysis revealed that the file behaves similarly to the one in the email sent to the targeted agency. It creates a folder (c:\windows\tasks) and drops config and PE files into it. A dropped executable file, unio.exe, is identical to the legitimate signed Logitech file disguised as Cannondriver.exe, described earlier in this blog. The unio.exe loads one of the other dropped files in the attack we are investigating, LBTServ.dll. In this case, LBTServ.dll contains the full backdoor payload instead of loading a shellcode to download it. This LBTServ.dll file also takes advantage of DLL Search Order Hijacking, has eight fake exports, and has a malicious export also named LGBT_Launch. This led us to believe that both attacks most likely came from the threat actor but in a different campaign that likely occurred in January 2022 based on the file submission date to VirusTotal.

More interestingly, the compilation time of 719f25e1fea12c8dc573e7161458ce7a5b6683dee3a49bb21a3ec838d0b35dd3 is “2016-07-09 12:49:34 UTC” while the compilation time of its dropper (SHA2: cdf417e67b0aaf798ac7c0f9ccb8b5b21f09b408ee6748beea5e03e76902e7fe) is about 29 seconds later, at 2016-07-09 13:18:11 UTC. These indicate this attacker group has been active since at least mid-2016.

A Tale of PivNoxy and Chinoxy Puppeter

We will now look at a partial history of the techniques used by this threat actor. Specifically, we will focus on their use of a file best described as the Logitech Bluetooth Wizard Host Process. This legitimately signed file contains a DLL Search Order hijacking vulnerability. The APT group takes advantage of this vulnerability by creating their own malicious “LBTServ.dll” file to be loaded whenever the real Logitech process is executed. Over time, this malicious DLL has evolved to use different techniques. The attack chain usually starts with an email containing an attachment. The attachment itself contains an executable that, when executed, drops the malicious DLL, the legitimate Logitech executable, and any associated files used by the malware.

Below is a timeline of dropper malware used by the threat actor utilizing the technique described above to deliver Chinoxy, PivNoxy, and recent Chinoxy variants.

Figure 7. Sample timeline of dropper malware based on file compilation time Note: Q1, Q2, Q3, and Q4 refer to January to March, April to June, July to September, and October to December, respectively.

As seen in the timeline, in Q3 of 2021, the threat actor switched their arsenal from PivNoxy to a new variant of Chinoxy, which decrypts and loads shellcode from a file and downloads the next payload. The switch from Chinoxy to PivNoxy occurred sometime in Q2 2020.

FortiGuard Labs has documented that from the middle of 2016 to the end of 2018, “LBTServ.dll” was consistently used by the variant known as Chinoxy. In this form, the malicious DLL loads an external configuration file named “k1.ini.”

Figure 8. The configuration file used by Chinoxy

This configuration file typically contains a base64 string, which turns out to be the C2 server used by Chinoxy.

Figure 9. Base64 decoded value from the Chinoxy configuration file

The “Remark” field contains the approximate date of the attack. This Chinoxy DLL sample (SHA2: 719f25e1fea12c8dc573e7161458ce7a5b6683dee3a49bb21a3ec838d0b35dd3), according to its metadata, was compiled on Sat Jul 09 12:49:34 2016 GMT. The main dropper (SHA2: cdf417e67b0aaf798ac7c0f9ccb8b5b21f09b408ee6748beea5e03e76902e7fe) itself was compiled on 2016-07-09 13:18:11 GMT. The turnaround time appears to have only been a few days. Chinoxy operated as a backdoor and collected data from the infected computers. It is interesting to note that the same C2 server was used for over two years. Our telemetry indicates that an overwhelming majority of the traffic to this server originated from India.

Things stayed relatively quiet until the end of 2020 and beginning of 2021 when the group decided to return. Operation Nightscout started targeting gamers in Southeast Asia. NoxPlayer is an Android emulator and, like many programs, contacts servers to check for updates. Instead of delivering their malware through email attachments, however, the APT group changed tactics and somehow compromised the update chain of NoxPlayer. A fake update package was sent to Southeast Asian gamers.

Similar to the Chinoxy case, this PivNoxy variant (SHA2: 5c2a6b11d876c5bad520ff9e79be44dfbb05ee6a6ff300e8427deab35085bef6) uses a fake update package to unpack several files, including files that abuse the same DLL Search Order Hijacking technique used against Logitech. However, in this case, “LBTServ.dll” was used to deliver malware more powerful than the previous iteration, with PivNoxy delivering the PoisonIvy RAT through the malicious DLL. While other vendors report infected computers were gamers from Southeast Asia, our telemetry suggests more infected gamers originated from Mexico.

At this point, this threat actor once again decided to go quiet. But fast forward to May 2022, and the spearphishing email disguised to come from a governmental division of Pakistan was sent to a telecommunication organization in South Asia. And this time, it attempted to deliver a new Chinoxy malware variant.

Regional Interest

The dropper malware covered earlier in this blog (SHA2: cdf417e67b0aaf798ac7c0f9ccb8b5b21f09b408ee6748beea5e03e76902e7fe) reaches out to goog1eupdate[.]com. Based on FortiGuard telemetry gathered over the past six months, almost 70% of the connections to the domain were made from Mexico, followed by 22% from India. Chinoxy variants also used this domain from 2016 to 2018.

We also found three similar samples connect to frontbeauty[.]dynamic-dns[.]net, beautygirl[.]dynamic-dns[.]net, and 784kjsuj[.]dynamic-dns[.]net. Over the same past six months, all access to the three domains was made from India. As they are dynamic DNS, not all connections can be considered related to the threat actor. However, a Bitdefender report published in November 2020 references the domain “goog1eupdate[.]com” as part of the IOCs for an APT group that uses the FunnyDream backdoor as part of their toolset and who primarily targeted South-Eastern Asia. Access to another C2 address, “mfaupdate[.]com”, was mainly observed from Mexico and India, while “ru[.]mst[.]dns-cloud[.]net” was primarily accessed from Israel and Ukraine. According to security researcher Sebastien Larinier, ru[.]mst[.]dns-cloud[.]net was used by a threat actor who targeted Kirghizstan. Further, a research blog released by NTT Security lists another C2 server, “eofficeupdating[.]com“, as being used by this threat actor as a C2 server for Smanager malware, which was used against Vietnam. NTT Security attributed Smanager to an unknown Panda group. Panda is typically part of the monikers used by Chinese threat actors, such as Deep Panda and Goblin Panda.

This evidence indicates that the threat group we are after has a particular interest not only in South-East Asia but also in South and Central Asia and potentially Mexico. Or at the least, they have a relationship with an attacker with interests there.

Conclusion

The attack against a telecommunications agency in South Asia began with a simple email that initially appeared to be a standard malicious spam email message. However, the attached Word doc was weaponized using a malicious tool, Royal Road, and is equipped with an exploit for an Equation Editor vulnerability (CVE-2018-0798). While a payload was unavailable at the time of the investigation, OSINT research points to the Poison Ivy RAT, which FortiGuard Labs has previously highlighted.

Based on our analysis, Asian organizations, and potentially some in Mexico, were a reconnaissance target of a threat actor that we believe was also involved in Operation NightScout in 2021. This threat actor, who uses Chinoxy and PivNoxy in their arsenal, has been active since at least mid-2016.

Fortinet Protections

The following (AV) signatures detect the samples mentioned in this blog:

Older Chinoxy variants

- W32/Chinoxy.AP!tr
- W32/Chinoxy.Z!tr
- W32/Generic.AC.433BE8
- W32/PossibleThreat

PivNoxy

- W32/Kryptik.HHBQ!tr
- W32/Injector.KR!tr
- W32/Rekvex.IY!tr
- W32/PossibleThreat

Newer Chinoxy variants

- W32/ERUG!tr
- W32/PossibleThreat

Older Chinoxy dropper

- W32/Chinoxy.AA!tr
- W32/Agent.BJWZYI!tr
- W32/Daws.DIGU!tr
- W32/Daws.EKFE!tr
- W32/Daws.EQVO!tr
- W32/Generic.AC.433BE8
- W32/Kryptik.GQMK!tr
- W32/RENOS.SM1!tr
- W32/Zuguo.A!tr
- RTF/CVE_2017_11882.A!exploit

PivNoxy dropper

- W32/Agent.SMC!tr
- W32/Generik.CIJIXOM!tr
- W32/Injector.KR!tr
- W32/Injector.SMC!tr
- W32/Kryptik.HHBQ!tr
- W32/Rekvex.IY!tr
- W32/Rekvex.JOHUGYE!tr
- W32/Rekvex.JOHUGYE!tr

- W32/RENOS.SM1!tr
- W32/Zuguo.A!tr

Newer Chinoxy dropper

- W32/Agent.ADWJ!tr
- W32/ERUG!tr
- W32/PossibleThreat
- Malicious_Behavior.SB

All network-based URIs are blocked by the WebFiltering client.

Fortinet has multiple solutions designed to help train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

In addition to these protections, we suggest that organizations also have their end users go through our FREE NSE training: NSE 1 – Information Security Awareness. It includes a module on Internet threats designed to help end users learn how to identify and protect themselves from various types of phishing attacks.

IOCs

File IOCs

Older Chinoxy variants

- 719f25e1fea12c8dc573e7161458ce7a5b6683dee3a49bb21a3ec838d0b35dd3
- 75f7b6197d648eaa8263d23c8f9aa9224038259d25df073803929d6582ea27b1
- a33dcbd2ccf291ebd465bfcd6a9be10b3d6c0d89fa5ee0038a2e41fbd6c0397d
- 5137bc35b042c0ea2ad56f3b0e03191e840cce9e9dadb470d6a7a018f3a1a4fb
- b0ad5af44a0a07a2408e9a6b4e4a27e366aa64350ff60f398d1b8086172034f6
- a8c21cb9dea1c9bc62adcc6de4a73c7971ea797ab4fdb93320532647625e22ba
- 6f7f142089b1d2e48880f59362c7c50e5d193166bdd5e4b27318133e8fe27b2c
- 399563e798edd4a9e1a89209b1b350a4e1197786c23c0986a1a965446e7d5474
- a8c21cb9dea1c9bc62adcc6de4a73c7971ea797ab4fdb93320532647625e22ba

PivNoxy

- a638cce32a01f63febe2d21b02ef9f6f6c6c59e2107a043eb2ae547ff9a1d776
- 8ceb84e33db56092618f763771630b0759d7122d5df5afaeb4c1ebc9e72ed7f1

- a4cbae07c1d674d41c1297be4e0c19b2f138c2ef29db16b5edc528026dc4e717
- 6ab62f7cd1c4a00c200cd130afa7352bb6e536e324cb9ead13e01e54146bb112
- af7d3f46c32f4040dbfb6f85d6db1471e29c4a9290654d3f44351e316f05fba5
- a557eed41c5e021209c7e3a3eada10abf43e2bfabf930552b6cb7a4b7568b971
- d49c0d6113a9928486e35a7013d9c09a52743bd8fe84712e27c54fcac9b9e31e
- 53c7ab494527a8118f89ba99dea51b223f98e368e687f42d31925945b0282e87

Newer Chinoxy variants

- c8934c7b3187e48b1ee44fc2c8e1c3ab19850efc1e45383442cfe4b9b4a06d01
- d59278ff54d30176263deadcb7d21ba6f9b7eb1139e3dcd6f7ea534183f96c92

Chinoxy dropper

- cdf417e67b0aaf798ac7c0f9ccb8b5b21f09b408ee6748beea5e03e76902e7fe
- f8a8ccfa6426f27da75649dbef26213aae6137f726d29232e45e4183391016bf
- 9f93a50cadd762d36788ce1c8d5deb2d26e109f717f3e2d4d5c8f0d3344de725
- a8f1e7eccae75e840b1d6982b06ee322ceaed65ade23a10d17c8414e5a522110
- 6a8ba940d40be935ffc623b5fadfdb4537c1787fedf5889021b0ceb65dfa809d
- 59ea7516b2a028e5cad938534099f45b5d28f7cfa32d268a8bdcbe5f6320b5a6
- 07a37e52533bf26f5d506c69e748f479de5dcd416103f8d7a4a06c948e1051ad
- 152f95a5bdf549c5ca789d0dd99d635ee69cca6fe464ced5b39d0316707a4914
- 947760b4f6888637087414572 97d74810ad45e20e2c02d91b54b056716803777
- 3f21e0b3ef80fd9393c6e187311a78aee22738f510ed227397249157b131b890
- 3c9d802f617aab4c6973cef74d2509fea00ee8454681c40df09a4734946e5125
- 82f8cf41aa720e268ee0c6e43cd52512ea4a2f98a51844071e0faaf1eb13ce62

PivNoxy dropper

- 2bebd0989d1d8c6bb681217399281640521d61ce207f358a4340377898ed44c5
- 6485d76e645d2f7e27a20d072f07c282583f21ec42801de588193d01b591a957
- 8dfda79f7848a41f0a8f7a68096fcb6783ace3f3430ae3d7d05fed1ad4533fe0
- 86c563a8630150934ae7468e074f81914d26b978c32571ce9f4d9b349dc03349
- 72a7341805713327f09f881bc7184610ed28101bfbda93fd829d0d52978c22eb
- 4d9af80dad6dcdfe37931094c42296d53ef6d98b633db32503d7972fd7e0e3f6
- e537b6eb903d9bb9b3cb0e63f9fddf2afa0875af7558b5bec3c98cebf1452e01
- c25ae716a651c7c846871275bfde7188224628e3380fd6f256aacba1cb15ad61
- 289ce24d873986d607ab8e43f499be562fa4925d2b5be16bb31ce68a00b4020a
- f229239ed7665338961eec60a17bcca0fed1eb957b0e751dd991ce664140d79c
- 5c2a6b11d876c5bad520ff9e79be44dfbb05ee6a6ff300e8427deab35085bef6

Newer Chinoxy dropper

- ab49e15c0a0e4f977748faae36255889c2239cde847ed49304881c123b9a0e99
- 8d7d259ac375171c59ac81ba9a16949ac7277c8ed3841c229ce48def0358c96e

- a8d92ace0ea438759428877a32cd92f73790d86d0e3384317c04a9ae4ed30c55
- c44be5ed5c4bec2be72ce9737bde5a2d48fe5fb0ea235ddc61ba447b26642949
- d863f559ba323625f20721e910bf920ee73a5303f6edadbec2aa670b640e01c8
- f309b42845ca3e36e0bb6ec68f424a11ff8f77642afc3bd4425118dc0d2514e0

Network IOCs

- goog1eupdate[.]com
- myhost[.]camdvr[.]org
- mfaupdate[.]com
- eofficeupdating[.]com
- 58[.]64[.]184[.]201
- cdn[.]cloudistcdn[.]com
- q.cloudistcdn.com
- beautygirl[.]dynamic-dns[.]net
- 784kjsuj[.]dynamic-dns[.]net
- frontbeauty[.]dynamic-dns[.]net
- instructor[.]giize[.]com

MITRE

Resource Development	
T1854.004	Compromise Infrastructure: Server
Initial Access	
T1566.001	Phishing: Spearphishing Attachment
T1195.002	Phishing: Compromise Software Supply Chain
Execution	
T1203	Exploitation for Client Execution
T1053.005	Scheduled Task/Job: Scheduled Task
T1201.002	User Execution: Malicious File

T1543.003	Create or Modify System Process: Windows Service
Persistence	
T1574.001	Hijack Execution Flow: DLL Search Order Hijacking
T1053.005	Scheduled Task/Job: Scheduled Task
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder
T1547.014	Boot or Logon Autostart Execution: Active Setup
Privilege Escalation	
T1574.001	Hijack Execution Flow: DLL Search Order Hijacking
T1055.001	Process Injection: Dynamic-link Library Injection
T1053.005	Scheduled Task/Job: Scheduled Task
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder
T1547.014	Boot or Logon Autostart Execution: Active Setup
Defense Evasion	
T1140	Deobfuscate/Decode Files or Information
T1574.001	Hijack Execution Flow: DLL Search Order Hijacking
T1055.001	Process Injection: Dynamic-link Library Injection
T1112	Modify Registry

T1027	Obfuscated Files or Information
Credential Access	
T1056.001	Input Capture: Keylogging
Discovery	
T1010	Application Window Discovery
Collection	
T1005	Data from Local System
T1074.001	Data Staged: Local Data Staging
T1056.001	Input Capture: Keylogging
Command and Control	
T1573.001	Encrypted Channel: Symmetric Cryptography
T1105	Ingress Tool Transfer
Exfiltration	
T1041	Exfiltration Over C2 Channel

The FortiGuard Labs has released a new playbook on the threat malware family known as “Chinoxy” and “PivNoxy” as part of our role in the Cyber Threat Alliance. For more information regarding this series of adversary playbooks being created by CTA members, please visit the Cyber Threat Alliance Playbook Whitepaper.

Learn more about Fortinet’s FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.