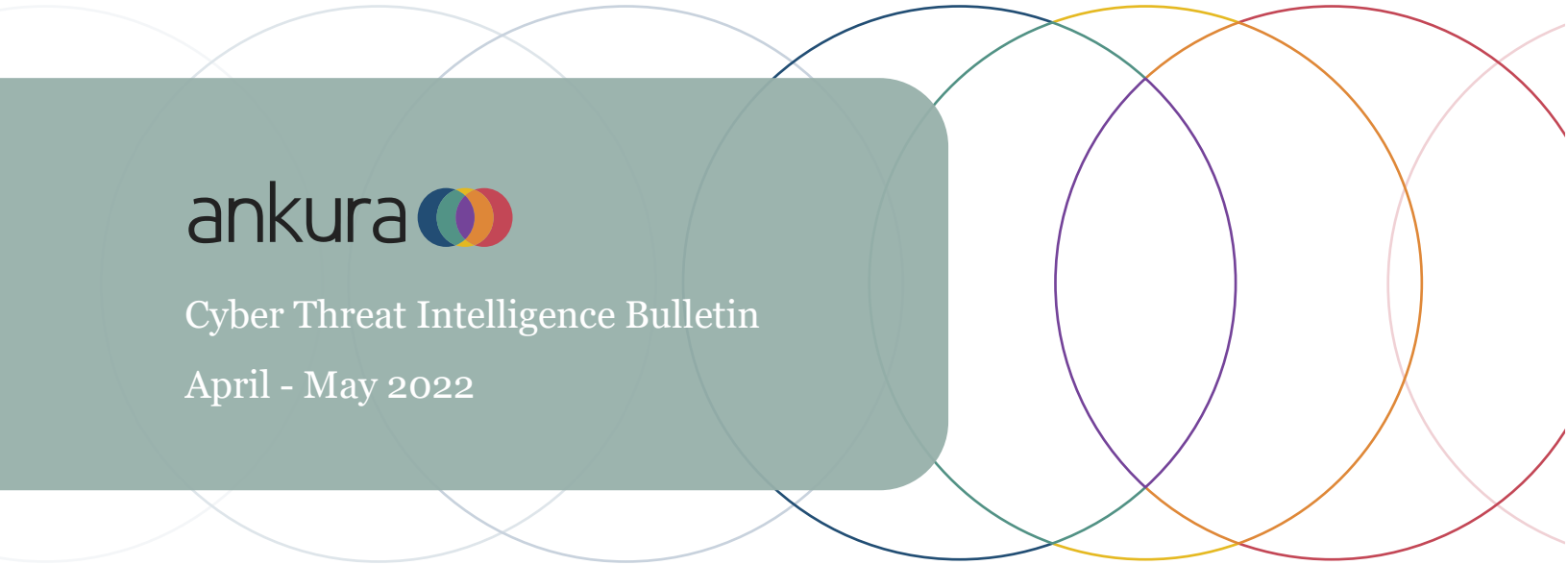


ankura

Cyber Threat Intelligence Bulletin

April - May 2022

Washington, DC
2000 K Street NW, 12th Floor
Washington, DC, United States 20006
+1.202.797.1111

Ankura Incident Response Services
Incident@ankura.com | 24/7 Assistance

TABLE OF CONTENTS

Executive Summary

Ankura's Cyber Threat Investigations and Expert Services (CTIX) team has compiled details of current cyber trends within the last sixty (60) days. This summary is intended to provide a medium depth of knowledge to high-level executives, technical analysts, and everyday readers who are looking to gain a deeper understanding of current, global threats.

This report will discuss the following in detail:

- CTIX analysts observed an operational uptick in Iranian state-sponsored threat actor behavior.
- One of the most prolific Russian ransomware groups, Conti, sets its crosshairs on Latin America as multiple Costa Rican government agencies suffer coordinated cyber-attacks.
- The tactics, techniques, and procedures (TTPs) of the North Korean state-sponsored Lazarus advanced persistent threat (APT) group.

GEOPOLITICAL TENSIONS LEAD TO INCREASE IN IRANIAN THREAT GROUP ACTIVITY

- Three well-known Iranian threat actors have been significantly more active in conducting cyberespionage campaigns over the past two months.
- Malicious Excel workbook attachment delivers new-and-improved version of the Saitama backdoor to Jordanian government in recent phishing campaign.
- DDoS attacks against Israel were conducted on the two-year anniversary of the death of Iranian commander Qasem Soleimani.

Summary

Since the beginning of May, Iranian threat actor activity has risen significantly across multiple organizations. Three separate Iranian groups, APT34, APT35, and Altahrea have stepped up their operations, targeting Jordan, Israel, the United States, and some European countries. CTIX analysts believe that this recent uptick in Iranian activity stems from the geopolitical tensions surrounding the war in Ukraine, and threat actors worldwide have been significantly more active.

APT34, also known as Cobalt Gypsy, Helix Kitten, Chrysene, and OilRig, has been leveraging extensive phishing campaigns against surrounding Middle Eastern countries and some international targets. APT34, whose first appearance was in 2014, has historically engaged in cyberespionage against telecommunications, energy, government, financial, and chemical industries on behalf of the Iranian government. In a recent APT34 phishing campaign, threat actors distributed malicious emails to Jordanian government employees with the intent of delivering a modernized version of the Saitama backdoor[1]. The Saitama payload was delivered through enabled macros within an Excel workbook attached to the phishing email. Once the user enabled content, the payload was loaded and executed on the system. The malware then stealthily communicated with actor-controlled command-and-control (C2) nodes every six (6) to eight (8) hours, utilizing the DNS protocol to mask communication streams.

[1] https://blog.malwarebytes.com/threat-intelligence/2022/05/apt34-targets-jordan-government-using-new-saitama-backdoor/

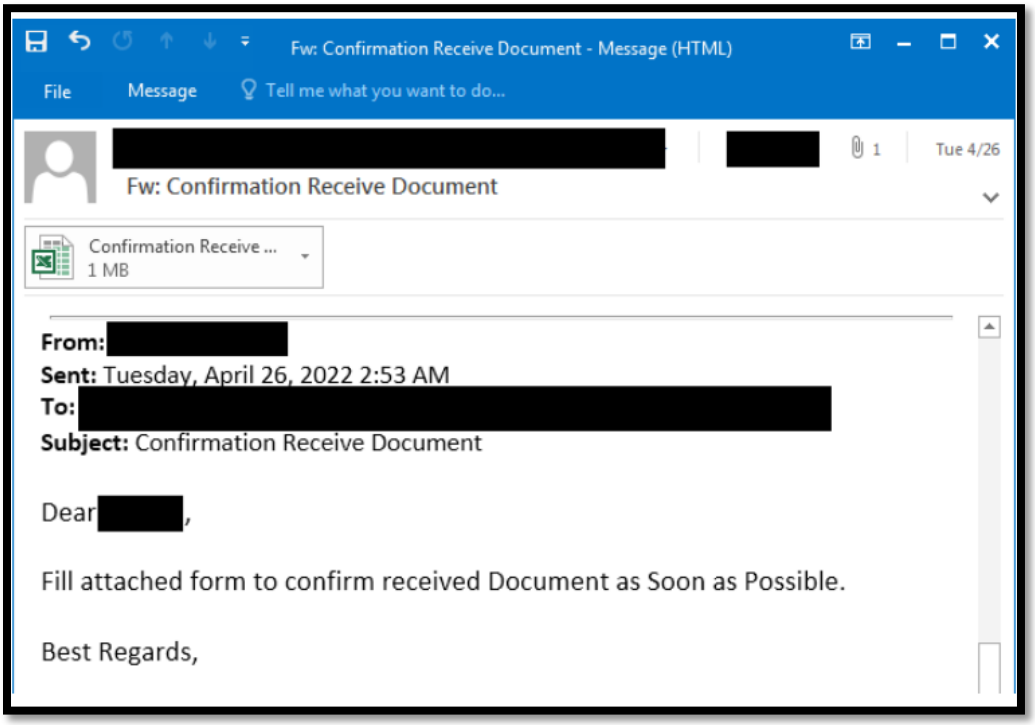
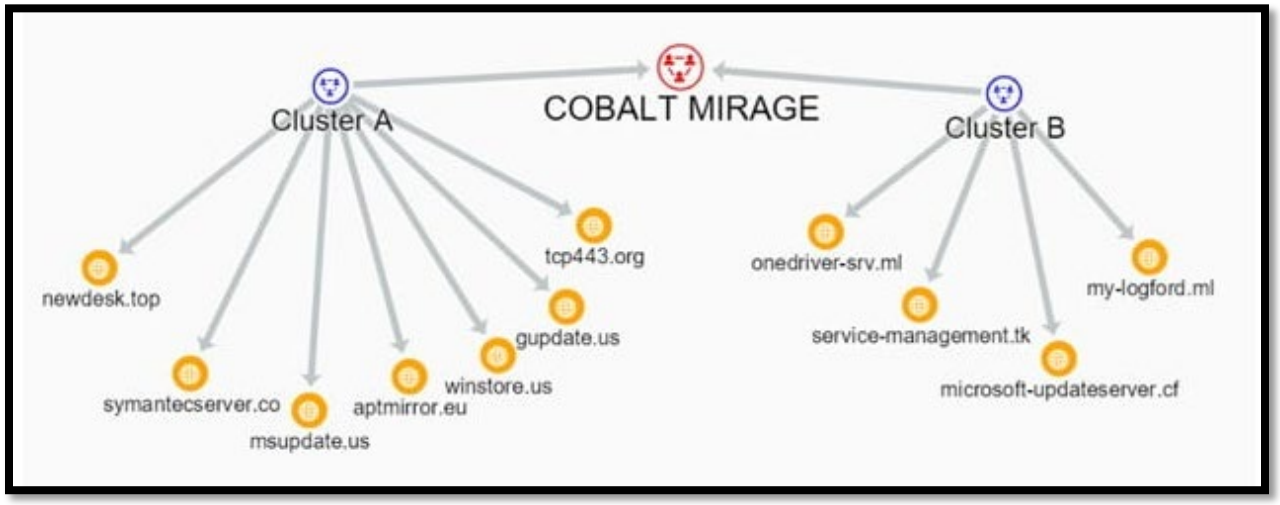


Figure 1: Phishing campaign email[2]

APT35, also known as Cobalt Mirage, Charming Kitten, and Phosphorus, has also increased its operations over the past eight (8) to ten (10) weeks. Cobalt Mirage threat actors generally use phishing campaigns to compromise their targets in hopes of exfiltrating data and posting it on their leak site. Recently, threat actors divided into two (2) groups and launched multiple ransomware campaigns throughout the United States, Australia, and Europe in hopes of achieving financial gain[3]. The first group was responsible for infiltrating and deploying ransomware onto the target while the second was responsible for intruding further to gain additional insight and intelligence.



[2] https://www.fortinet.com/blog/threat-research/please-confirm-you-received-our-apt
[3] https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us

Figure 2: Visual representation of two Cobalt Mirage groups in ransomware campaign[4]

Once infiltrated, Cobalt Mirage actors performed heavy reconnaissance on their targets, specifically on Microsoft Exchange and Fortinet ports (4443, 8443, 10443). Post-recon, Cobalt Mirage actors exploit system vulnerabilities in FortiGate SSL (CVE-2019-5591), FortiOS SSL VPN (CVE-2020-12812), FortiOS (CVE-2018-13379), and the attack chain ProxyShell (CVE-2021-31207, CVE-2021-34523, CVE-2021-34473). Once fully intruded into the system, depending on the sub-group that compromised the target, either ransomware will be deployed onto the network or threat actors will exfiltrate data from the entity for cyber espionage purposes.

Lastly, the Altahrea team, another Iranian-backed organization, targeted the website infrastructure of the Israel Airports Authority (IAA)[5] on April 20th, 2022. Altahrea conducted a Distributed Denial of Service (DDoS) attack against IAA servers, in which there was no resulting harm. In addition to the IAA website DDoS attack, there were additional DDoS attacks by the Altahrea team on several Israeli entities, including an Israeli news network, the Civil Authority of Israel, and the KAN Israeli Public Broadcasting Corporation, that did not have any significant impact to critical business processes. The timing of these attacks, the two (2) year anniversary of the death of Iranian commander Qasem Soleimani in an air strike, suggests they are politically motivated. After observing the trends of Iranian threat actor behavior, CTIX analysts predict that throughout 2022 there will be waves of increased phishing and DDoS attacks that span weeks or months. This will be followed by small hiatuses where the groups back off from the limelight for many reasons that include planning future attacks, and recruiting insiders, as well as simply just letting off pressure from the authorities.

[4] https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us
[5] https://nsi-globalcounterintelligence.com/cyber-security/pro-iran-hackers-target-israel-airports-authority-website/

CONTI CONDUCTS RANSOMWARE ATTACK AGAINST COSTA RICA

- Coordinated ransomware attack forced Costa Rican leadership to declare a national state of emergency.
- Conti released 672 GB of data after the Costa Rican government declined to pay a $10M ransom.
- United States government is offering a $15M reward for information leading to the identification, capture, and prosecution of Conti members.

Summary

On May 8th, 2022, newly sworn in Costa Rican president Rodrigo Chavez declared a national emergency and stated the country was "at war" with the ransomware group Conti (also known as threat actor UNC1756).[6] Chavez's announcement followed cyberattacks on a number of Costa Rican government agencies, including the Costa Rican Social Security Fund, The Ministry of Science, The National Meteorological Institute, and The Costa Rican Finance Ministry. Since the attacks started in April, the number of national institutions impacted has risen to twenty-seven (27).[7] After the Costa Rican government declined to pay a $10 million ransom, Conti released 672 gigabytes (GB) of data purportedly stolen in the ransomware attack. Despite leaking the information anyway, Conti followed up with a second request, this time for $20 million and announced their goal was to overthrow the government. The full impact of the disruption of Costa Rican government services is not yet known, but one (1) significant impact has been to their Treasury agency, as they cannot issue signatures or stamps digitally at this time. This appears to play into a new kind of antagonism for Conti as they later posted the following message regarding their involvement in the Costa Rica attacks as well as claiming credit for an attack on Oregon election finance infrastructure.

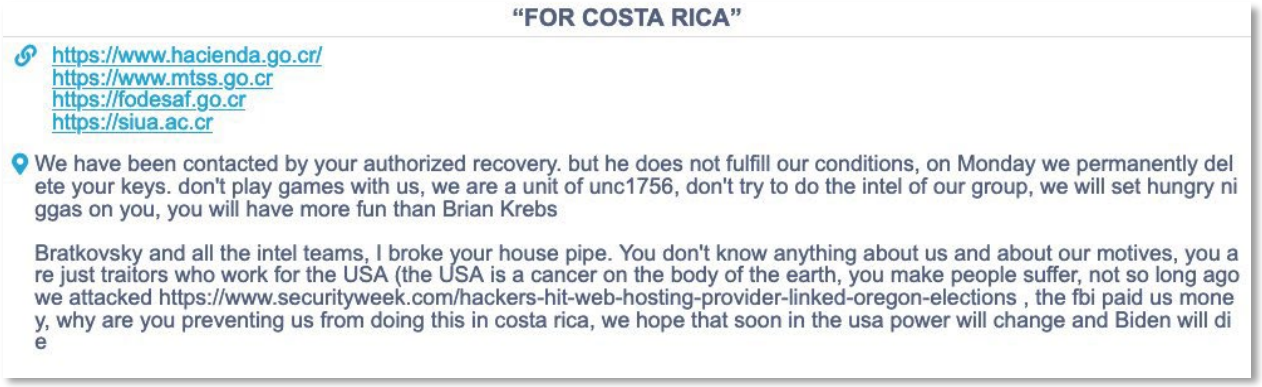


Figure 3: Conti's Leak Site Posting Regarding Costa Rica

Researchers and the Costa Rican government are debating whether Conti actually had insider help with the attack, despite Conti's claim of having done so.[8] Researchers noted that the moniker associated with the attack was created and active for only about one (1) month before the attacks, which is a relatively short period of time to target and recruit an appropriately placed insider. Also up for debate are Conti's motivations for the attack on Costa Rica. Some speculate it is linked to Russia's invasion of Ukraine and Costa Rica's (and the rest of the West) backing of Ukrainian military operations. That said, Conti has historically been primarily financially motivated, and some assess that their rhetoric about overthrowing the government

[6] https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/
[7] https://techcrunch.com/2022/05/20/costa-rica-ransomware-attack/
[8] https://techcrunch.com/2022/05/20/costa-rica-ransomware-attack/

might be a tactic to compel the public to urge the government to pay the ransom. In any event, this attack by Conti demonstrates a shift toward Latin America and smaller regions that typically have less defensive cyber infrastructure. In response to this and other attacks, the United States increased its own efforts to combat Conti, offering $15M in rewards for information leading to the identification, capture, and prosecution of Conti actors.[9]

[9] https://www.speartip.com/resources/us-offering-15-million-for-information-on-conti-ransomware-group/

THREAT ACTOR OF THE MONTH

- The Lazarus Group is a financially motivated North Korean state-sponsored APT.
- The group has been increasingly active in targeting cryptocurrency start-ups.
- Four strains of ransomware targeting the APAC region have been attributed to the group.

Summary:

The Lazarus Group is a North Korean state-sponsored advance persistent threat (APT) group that has been operational since at least 2009 and is known to consist of various clusters. Lazarus Group clusters can act differently, but there is enough overlap that analysts often attribute any North Korean state-sponsored actor to Lazarus. The Lazarus Group was first brought to the public eye in 2014 for its destructive attack against Sony Pictures Entertainment. Following the creation of the movie "The Interview," a parody depicting North Korea in an unflattering light, the Lazarus Group (calling themselves "Guardians of Peace"[10]) deployed wiper malware across Sony, taking down business critical systems and disrupting the release of the movie. This attack was easily attributable to North Korea because, in addition to their clear motive to disrupt that specific movie, the FBI confirmed that the infrastructure used in the attack has been attributed to Lazarus and investigators identified snippets of the analyzed WannaCry ransomware source code that only appear in malware that has been used by or attributed to the Lazarus Group. The ransomware devastated organizations in 2017 and the Lazarus-attributed backdoor "Contopee" was also shown to have code similarities to the WannaCry ransomware.[11] In 2016, the Lazarus Group cluster BlueNoroff attempted to raid $1 billion through a digital bank heist targeting the Bangladesh Central Bank. They were almost successful but were ultimately foiled when all but one of the transactions were halted due to various small mistakes on the part of the hackers.[12] Unlike the Sony hack, the attack on the Bangladesh Central Bank appeared to have no motive other than financial gain. Following the attack, the group began to target financial institutions, casinos, financial software companies, and cryptocurrency businesses across the US, Australia, India, Mexico, Norway, Russia, and other countries around the world. These two (2) high-profile attacks highlight the new objective of attacks conducted by the Lazarus Group: stealing money through heists and ransomware.

BlueNoroff

In the first half of 2022, the Lazarus cluster BlueNoroff has been increasingly active. BlueNoroff has been observed targeting cryptocurrency start-ups using targeted phishing in a campaign named "SnatchCrypto." Targeting small cryptocurrency start-ups with often underdeveloped security gives the group easy initial access into the organizations' networks and a lot of time to surveil before being detected. Before conducting an attack, BlueNoroff stalks its target for months to gather information, then strikes with a phishing email with a fake Google Drive document attachment. The group has two (2) malware droppers it delivers as the attached document.[13] The first is a ZIP file containing a password-protected word document as well as a "Password.txt.lnk" file that uses the .LNK shortcut file type to launch Visual Basic and PowerShell scripts to deploy a fully featured backdoor. The second dropper is a malicious word document with an embedded Visual Basic Script that downloads a stager to deploy the same backdoor. Once initial access into an organization is gained, BlueNoroff uses keystroke logging and attempts to replace common cryptocurrency wallet browser extensions to monitor transactions. Utilizing these techniques allows the group to steal large

[10] https://www.fbi.gov/news/press-releases/press-releases/update-on-sony-investigation
[11] https://securelist.com/wannacry-and-lazarus-group-the-missing-link/78431/
[12] https://www.bbc.com/news/stories-57520169
[13] https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/

amounts of cryptocurrency with little effort, achieving their goal of generating profits for the North Korean government.

Deploying Ransomware Across Asia

While BlueNoroff has focused on cryptocurrency organizations, a separate and currently unidentified Lazarus cluster has been increasingly experimenting with ransomware. Ransomware is not a new attack vector for the Lazarus Group, with some samples dating back to 2009[14] and the attribution of the WannaCry worm in 2017[15]. The new developments have arisen in their targeting of the Asia Pacific (APAC) region and began with the "Tflower" ransomware, a malware that is deployed using the Lazarus Groups signature "MATA" framework. The MATA framework allows easy development, deployment, and communication between a piece of malware and its command-and-control (C2) server.[16] The MATA framework is developed and used solely by Lazarus operators, providing direct attribution between Tflower and the Lazarus Group. Following Tflower, an additional ransomware emerged using the same MATA framework, dubbed "VHD" ransomware. The new ransomware proved interesting to Trellix researchers when, after conducting code similarity analysis, they discovered four (4) other previously unattributed ransomware strains linking back to VHD: "BEAF", "PXJ", "ZZZZ", and "ChiChi" ransomware.[17] According to the Trellix researchers, VHD directly shares code with BEAF, ZZZ, and PXJ.

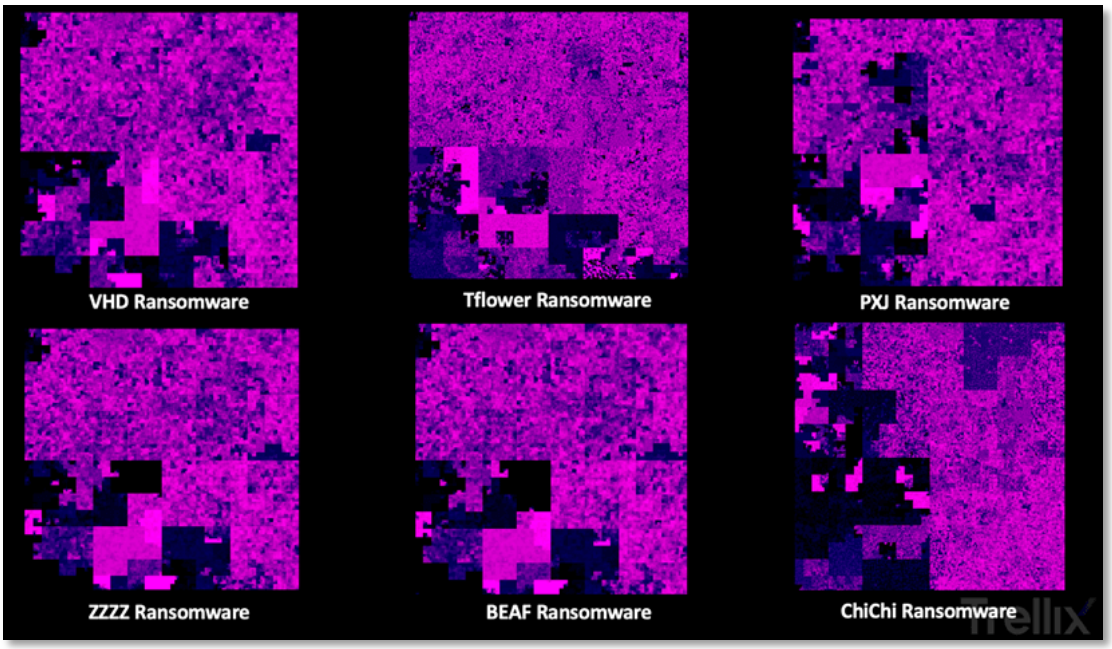


Figure 4: Visual depictions of the ransomware code using Hilbert curve graphs[18]

Using code visualization techniques, the researchers identified multiple obvious overlaps between the four (4) ransomware families. By analyzing the ransomware notes dropped by the malware, the researchers discovered the same email address was used in both the CHiCHi and ZZZZ ransom notes.

---

[14] https://www.intezer.com/blog/research/examining-code-reuse-reveals-undiscovered-links-among-north-koreas-malware-families/
[15] https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537
[16] https://usa.kaspersky.com/blog/mata-framework/22890/
[17] https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/the-hermit-kingdoms-ransomware-play.html
[18] https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/the-hermit-kingdoms-ransomware-play.html

The discoveries of the ransomware strains lead to interesting questions. In an age where ransomware is organized through large enterprise-like operations, it begs the question of why the Lazarus Group wants to create small-time ransomware strains. One explanation could be the requirement for stealth in Lazarus operations. Excluding WannaCry, their ransomware mainly targets the APAC region, a notoriously underreported region for ransomware. On top of that, always developing new ransomware prevents the few researchers studying the region from fully realizing the extent of the Lazarus Group's ransomware campaign. The Lazarus Group has been shown to be one of the most persistent financially motivated threat actors in the world and will likely continue to do so as long as they continue to be successful.

Trending IOCs

The following technical indicators of compromise (IOCs) are associated with monitored threat groups and/or campaigns of interest within the past sixty (60) days. IOCs can be utilized by organizations to detect security incidents more quickly and easily, as indicators may not have otherwise been flagged as suspicious or malicious.

Indicator	Type	Attribution
118.70.116[.]154:8080	IP Address	BlueNoroff
163.25.24[.]44	IP Address	BlueNoroff
45.238.25[.]2	IP Address	BlueNoroff
doc.filesaves[.]cloud	Domain	BlueNoroff
abiesvc[.]com	Domain	BlueNoroff
abiesvc[.]info	Domain	BlueNoroff
abiesvc.jp[.]net	Domain	BlueNoroff
atom.publicvm[.]com	Domain	BlueNoroff
att.gdrvupload[.]xyz	Domain	BlueNoroff
authenticate.azure-drive[.]com	Domain	BlueNoroff
azureprotect[.]xyz	Domain	BlueNoroff
backup.163qiye[.]top	Domain	BlueNoroff
beenos[.]biz	Domain	BlueNoroff
bhomes[.]cc	Domain	BlueNoroff
bitcoinnews.mefound[.]com	Domain	BlueNoroff
bitflyer[.]team	Domain	BlueNoroff
blog.cloudsecure[.]space	Domain	BlueNoroff
buidihub[.]com	Domain	BlueNoroff
chemistryworld[.]us	Domain	BlueNoroff
circlecapital[.]us	Domain	BlueNoroff
client.googleapis[.]online	Domain	BlueNoroff
cloud.azure-service[.]com	Domain	BlueNoroff
cloud.globalbrains[.]co	Domain	BlueNoroff
cloud.jumpshare[.]vip	Domain	BlueNoroff
cloud.venturelabo[.]co	Domain	BlueNoroff
cloudshare.jumpshare[.]vip	Domain	BlueNoroff
coin-squad[.]co	Domain	BlueNoroff
coinbig[.]dev	Domain	BlueNoroff
coinbigex[.]com	Domain	BlueNoroff
deepmind[.]fund	Domain	BlueNoroff
dekryptcap[.]digital	Domain	BlueNoroff
dllhost[.]xyz:5600	Domain	BlueNoroff
doc.venturelabo[.]co	Domain	BlueNoroff
doc.youbicapital[.]cc	Domain	BlueNoroff
doconline[.]top	Domain	BlueNoroff

docs.azureword[.]com	Domain	BlueNoroff
docs.coinbigex[.]com	Domain	BlueNoroff
docs.gdriveshare[.]top	Domain	BlueNoroff
docs.goglesheet[.]com	Domain	BlueNoroff
docs.securedigitalmarkets[.]co	Domain	BlueNoroff
docstream[.]online	Domain	BlueNoroff
document.antcapital[.]us	Domain	BlueNoroff
document.bhomes[.]cc	Domain	BlueNoroff
document.fastercapital[.]cc	Domain	BlueNoroff
document.kraken-dev[.]com	Domain	BlueNoroff
document.lundbergs[.]cc	Domain	BlueNoroff
document.skandiafastigheter[.]cc	Domain	BlueNoroff
documentprotect[.]live	Domain	BlueNoroff
documentprotect[.]pro	Domain	BlueNoroff
documents.antcapital[.]us	Domain	BlueNoroff
docuserver[.]xyz	Domain	BlueNoroff
domainhost.dynamic-dns[.]net	Domain	BlueNoroff
download.azure-safe[.]com	Domain	BlueNoroff
download.azure-service[.]com	Domain	BlueNoroff
download.gdriveupload[.]site	Domain	BlueNoroff
drives.googldrive[.]xyz	Domain	BlueNoroff
drives.googlecloud[.]live	Domain	BlueNoroff
driveshare.googldrive[.]xyz	Domain	BlueNoroff
dronefund[.]icu	Domain	BlueNoroff
drw[.]capital	Domain	BlueNoroff
eii[.]world	Domain	BlueNoroff
etherscan.mrslove[.]com	Domain	BlueNoroff
faq78.faqserv[.]com	Domain	BlueNoroff
fastdown[.]site	Domain	BlueNoroff
fastercapital[.]cc	Domain	BlueNoroff
file.venturelabo[.]co	Domain	BlueNoroff
filestream[.]download	Domain	BlueNoroff
foundico.mefound[.]com	Domain	BlueNoroff
galaxydigital[.]cc	Domain	BlueNoroff
galaxydigital[.]cloud	Domain	BlueNoroff
googledrive[.]download	Domain	BlueNoroff
googledrive[.]email	Domain	BlueNoroff
googledrive[.]online	Domain	BlueNoroff
googledrive.publicvm[.]com	Domain	BlueNoroff
googleexplore[.]net	Domain	BlueNoroff
googleservice[.]icu	Domain	BlueNoroff
googleservice[.]xyz	Domain	BlueNoroff
gsheet.gdocsdown[.]com	Domain	BlueNoroff

hiccup[.]shop	Domain	BlueNoroff
innoenergy[.]info	Domain	BlueNoroff
isosecurity[.]xyz	Domain	BlueNoroff
jack710[.]club	Domain	BlueNoroff
jumpshare[.]vip	Domain	BlueNoroff
kraken-dev[.]com	Domain	BlueNoroff
ledgerservice.itsaol[.]com	Domain	BlueNoroff
lemniscap[.]cc	Domain	BlueNoroff
lundbergs[.]cc	Domain	BlueNoroff
mail.gdriveupload[.]info	Domain	BlueNoroff
mail.gmaildrive[.]site	Domain	BlueNoroff
mail.googleupload[.]info	Domain	BlueNoroff
mclland[.]com	Domain	BlueNoroff
microstratgey[.]com	Domain	BlueNoroff
miss.outletalertsdaily[.]com	Domain	BlueNoroff
msoffice.qooqle[.]download	Domain	BlueNoroff
note.onedocshare[.]com	Domain	BlueNoroff
onlinedocpage[.]org	Domain	BlueNoroff
page.googledocpage[.]com	Domain	BlueNoroff
product.onlinedoc[.]dev	Domain	BlueNoroff
protect.antcapital[.]us	Domain	BlueNoroff
protect.azure-drive[.]com	Domain	BlueNoroff
protect.venturelabo[.]co	Domain	BlueNoroff
protectoffice[.]club	Domain	BlueNoroff
pvset.itsaol[.]com	Domain	BlueNoroff
qooqle[.]download	Domain	BlueNoroff
qoqle[.]online	Domain	BlueNoroff
regcnlab[.]com	Domain	BlueNoroff
reit[.]live	Domain	BlueNoroff
securedigitalmarkets[.]ca	Domain	BlueNoroff
share.bloomcloud[.]org	Domain	BlueNoroff
share.devprocloud[.]com	Domain	BlueNoroff
share.docuserver[.]xyz	Domain	BlueNoroff
share.stablemarket[.]org	Domain	BlueNoroff
sharedocs[.]xyz	Domain	BlueNoroff
signverydn.sharebusiness[.]xyz	Domain	BlueNoroff
sinovationventures[.]co	Domain	BlueNoroff
skandiafastigheter[.]cc	Domain	BlueNoroff
slot0.regcnlab[.]com	Domain	BlueNoroff
svr04.faqserv[.]com	Domain	BlueNoroff
tokenhub.mefound[.]com	Domain	BlueNoroff
tokentrack.mrbasic[.]com	Domain	BlueNoroff
twosigma.publicvm[.]com	Domain	BlueNoroff

up.digifincx[.]com	Domain	BlueNoroff
upcraft[.]io	Domain	BlueNoroff
updatepool[.]online	Domain	BlueNoroff
upload.gdrives[.]best	Domain	BlueNoroff
venturelabo[.]co	Domain	BlueNoroff
verify.googleauth[.]pro	Domain	BlueNoroff
word.azureword[.]com	Domain	BlueNoroff
www.googledocpage[.]com	Domain	BlueNoroff
www.googlesheetpage[.]org	Domain	BlueNoroff
www.onlinedocpage[.]org	Domain	BlueNoroff
youbicapital[.]cc	Domain	BlueNoroff
85fe6affdb218b2d09a59e08e80eb1fa	Hash	BlueNoroff
de097c5ab5e31ac16b4466cd56e9bd2d	Hash	BlueNoroff
033609f8672303feb70a4c0f80243349	Hash	BlueNoroff
2100e6e585f0a2a43f47093b6fabde74	Hash	BlueNoroff
4a3de148b5df41a56bde78a5dcf41975	Hash	BlueNoroff
5af886030204952ae243eedd25dd43c4	Hash	BlueNoroff
5f761f9aa3c1a76b17f584b9547a01a7	Hash	BlueNoroff
7a4a0b0f82e63941713ffd97c127dac8	Hash	BlueNoroff
813203e18dc1cc8c70d36ed691ca0df3	Hash	BlueNoroff
961e6ec465d7354a8316393b30f9c6e9	Hash	BlueNoroff
9ea244f0a0a955e43293e640bb4ee646	Hash	BlueNoroff
a3c61de3938e7599c0199d2778f7d417	Hash	BlueNoroff
a5d4bfc3eab1a28ffbcba67625d8292e	Hash	BlueNoroff
a94529063c3acdbfa770657e9126b56d	Hash	BlueNoroff
ab095cb9bc84f37a0a655fbc00e5f50e	Hash	BlueNoroff
b52d30d1db40d5d3c375c4a7c8a115c1	Hash	BlueNoroff
dd2569684ca52ed176f1619ecbfa7aaa	Hash	BlueNoroff
dff21849756eca89ebfaa33ed3185d95	Hash	BlueNoroff
e18dd8e61c736cfc6fff86b07a352c12	Hash	BlueNoroff
e546b851ac4fa5a111d10f40260b1466	Hash	BlueNoroff
e6e64c511f935d31a8859e9f3147fe24	Hash	BlueNoroff
ea7ed84f7936d4cbafa7cec51fe39cf7	Hash	BlueNoroff
f414f6590636037a6ec92a4d951bdf55	Hash	BlueNoroff
4e207d6e930db4293a6d720cf47858fc	Hash	BlueNoroff
5e44deca6209e64f4093beae92db0c93	Hash	BlueNoroff
84c427e002fd162d596f3f43ce86fd6a	Hash	BlueNoroff
c16977fefbdc825a5c6760d2b4ea3914	Hash	BlueNoroff
e5d12ef32f9bd3235d0ac45013040589	Hash	BlueNoroff
09bca3ddbc55f22577d2f3a7fda22d1c	Hash	BlueNoroff
0eb71e4d2978547bd96221548548e9f0	Hash	BlueNoroff
da599b0cde613b5512c13f299fec739e	Hash	BlueNoroff
0c9170a2584ceeddb89e4c0f0a2353ed	Hash	BlueNoroff

5053103dd5d075c1dc54edf1f8568098	Hash	BlueNoroff
536bae311c99a4d46f503c68595d4431	Hash	BlueNoroff
3078265f207fed66470436da07343732	Hash	BlueNoroff
15f1ae1fed1b2ea71fdb9661823663c6	Hash	BlueNoroff
56fe283ca3e1c1667191cc7764c260b6	Hash	BlueNoroff
850751de7b8e158d86469d22ad1c3101	Hash	BlueNoroff
1a8282f73f393656996107b6ec038dd5	Hash	BlueNoroff
2ea2ceab1588810961d2fc545e2f957e	Hash	BlueNoroff
561f70411449b327e3f19d81bb2cea08	Hash	BlueNoroff
3812cdc4225182326b1425c9f3c2d50b	Hash	BlueNoroff
4274e6dbc2b7aee4ef080d19fff47ce7	Hash	BlueNoroff
427bdfe4425e6c8e3ea41d89a2f55870	Hash	BlueNoroff
7a83be17f4628459e120a64fcab70bac	Hash	BlueNoroff
5d662269739f1b81072e4c7e48972420	Hash	BlueNoroff
244a23172af8720882ae0141292f5c47	Hash	BlueNoroff
a8e2c94abb4c1e77068a5e2d8943296c	Hash	BlueNoroff
89c26cefa057cf21054e64b5560bf583	Hash	BlueNoroff
805949896d8609412732ee7bfb44900a	Hash	BlueNoroff
a2be99a5aa26155e6e42a17fbe4fd54d	Hash	BlueNoroff
28917b4187b3b181e750bf024c6adf70	Hash	BlueNoroff
9f8e51f4adc007bb0364dfafb19a8c11	Hash	BlueNoroff
790a21734604b374cf260d20770bfc96	Hash	BlueNoroff
db315d7b0d9e8c9ca0aa6892202d498b	Hash	BlueNoroff
02904e802b5dc2f85eec83e3c1948374	Hash	BlueNoroff
baebc60beaced775551ec23a691c3da6	Hash	BlueNoroff
302314d503ae88058cb4c33a6ac6b79b	Hash	BlueNoroff
aeac6f569fb9a7d3f32517aa16e430d6	Hash	BlueNoroff
926DEEAF253636521C26442938013204	Hash	BlueNoroff
8064e00b931c1cab6ba329d665ea599c	Hash	BlueNoroff
bcb4a8f190f2124be57496649078e0ae	Hash	BlueNoroff
781a20f27b72c1c901164ce1d025f641	Hash	BlueNoroff
483e3e0b1dceb4a5a13de65d3556c3fe	Hash	BlueNoroff
DACM Opportunities.gdoc.lnk	Filename	BlueNoroff
პაროლი.lnk	Filename	BlueNoroff
Password.txt.lnk	Filename	BlueNoroff
Security Bugs in rigs.pdf.lnk	Filename	BlueNoroff
Xbox.lnk	Filename	BlueNoroff
Readme.txt.lnk	Filename	BlueNoroff
UserAssist.lnk	Filename	BlueNoroff
Anri	Text	BlueNoroff - Front Company
Beenos	Text	BlueNoroff - Front Company

CoinSquad	Text	BlueNoroff - Front Company
Daiwa Corporate Investment	Text	BlueNoroff - Front Company
Dekrypt Capital	Text	BlueNoroff - Front Company
Emurgo	Text	BlueNoroff - Front Company
Youbi Capital	Text	BlueNoroff - Front Company
Global Brain	Text	BlueNoroff - Front Company
Sinovation Ventures	Text	BlueNoroff - Front Company
Abies Ventures	Text	BlueNoroff - Front Company
Lemniscap	Text	BlueNoroff - Front Company
Coinbig	Text	BlueNoroff - Front Company
Secure Digital Markets	Text	BlueNoroff - Front Company
Ant Capital Partners	Text	BlueNoroff - Front Company