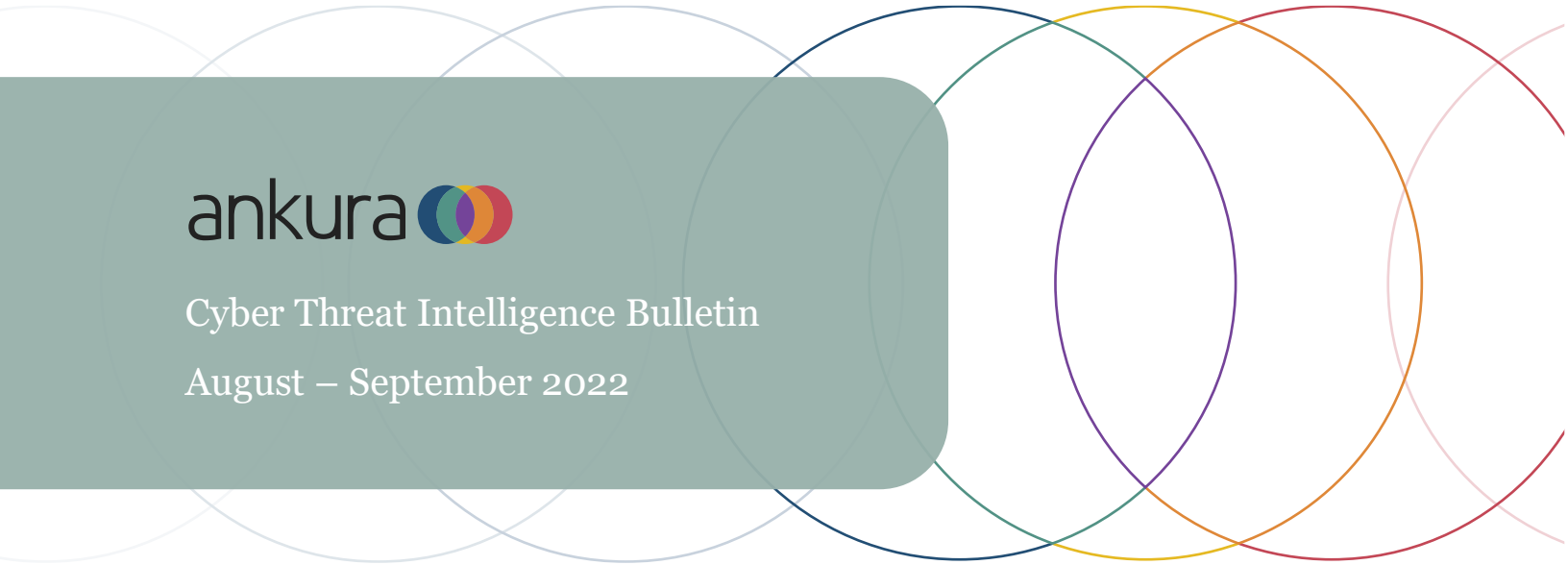

ankura

Cyber Threat Intelligence Bulletin

August – September 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:

- Researchers from Recorded Future provide a methodology for using aggregated threat-intelligence to assist them in tracking and prosecuting human sex traffickers.
- An emerging threat actor known as "Monti" has made waves with very similar TTPs to the infamous threat actor "Conti".
- "Homeland Justice", a threat organization with ties to the Iranian state, has launched a catastrophic attack campaign against the government of the NATO-member Albania.
- A courtroom debate in the US regarding the ethics of allowing state and private entities to pay ransomware demands is currently underway, after states like North Carolina and Florida introduce legislation that could make cyber extortion a far less profitable enterprise for threat actors.
- "Worok", a new cluster of the Chinese state-affiliated threat group TA428, has been observed targeting military sector organizations in Eastern Europe and Afghanistan with new custom malware.

SUPPORTING LAW ENFORCEMENT EFFORTS WITH THREAT INTELLIGENCE TO PROSECUTE HUMAN TRAFFICKERS

- Recorded Future's Insikt Group published a report on actively monitoring adult classified websites to assist law enforcement with prosecuting human sex traffickers.
- Suspect sites use a similar model to the former Backpage website, seized by the US Department of Justice in 2018.
- Investigators monitor suspected human trafficking sources to create massive datasets that can be quickly queried by law enforcement, exponentially boosting the investigative speed and capabilities for combatting human sex trafficking.

Summary

In the age of high-speed internet and social media, criminals have evolved to use information technology to bolster their criminal enterprises and human traffickers are no different. Whether it be through the clearnet or dark web, human traffickers have leveraged the internet to scale their operations, forcing law enforcement to reevaluate how to best combat this problem. In response to the changes in trafficker tactics, techniques, and procedures (TTPs), governments across the world have responded with legislation and policies in an attempt to better thwart the efforts of these criminals. Researchers from Recorded Future's Insikt Group have published compelling reports as a proof-of-concept (PoC) for a methodology on how law enforcement agencies and investigators can utilize real-time threat intelligence to leverage sources of data in order to aid in tracking, mitigating, and potentially prosecuting human sex traffickers. The Insikt Group report is the second part in a four (4) part series, with the first focusing on how to prevent human sex trafficking.

According to the Human Trafficking Institute, a 2017 study from the International Labour Organization (ILO) titled "Global estimates of modern slavery: Forced labour and forced marriage" estimated that there were 24.9 million victims of human trafficking in 2016. This number included both sex trafficking and commercial sexual exploitation, as well as individuals being exploited for forced labor.[1] Of the 24.9 million victims, approximately 4.8 million were victims of sex trafficking for commercial sexual exploitation. Out of the 4.8 million victims, 3.8 million were adults and 1 million were children, with 99% of those impacted being women and girls.**Error! Bookmark not defined.**

In this latest analysis,[2] the Insikt Group researchers focused on criminals active in one (1) aspect/space of human sex trafficking, which is the use of adult classified webpages. These websites are similar in format and intent to the infamous backpage[.]com, which was a website for advertising goods and services much like Craigslist, except the services offered on Backpage were classified. In 2018, Backpage was seized by the US Department of Justice on charges related to prostitution and human sex trafficking. With Backpage taken down, traffickers capitalizing on their "classified services" listings had to adapt, giving birth to many more similar webpages. Many of the sites are designed based off of a Backpage source code clone, and others use the term "Backpage" in their website branding or as part of their site domain. These websites, although similar in style and features, offer a plethora of different services, many of which seem benign at first glance. The services include massage parlor forums, on-demand maid services, babysitting services, escort services, and many more.

[1] https://traffickinginstitute.org/breaking-down-global-estimates-of-human-trafficking-human-trafficking-awareness-month-2022/
[2] https://www.recordedfuture.com/combating-human-trafficking-with-threat-intelligence-for-prosecution

Figure 1. Redacted adult classified webpage code indicating Backpage clone

The Insikt Group analyzed eight (8) "Backpage-like,"[2] websites, aggregating the data of more than 66,000 individual posts. The researchers identified tens of thousands of phone numbers and email addresses. Many of them were found to be unique and overwhelmingly attributed to the US, with only four (4) of the websites offering international sections. Along with the gathering of phone numbers and emails, Insikt researchers also parsed each post to identify key terms associated with human sex trafficking as well as the mentioning of locations like countries, states, and cities. All of this data was then combined into datasets which could be queried by researchers to identify trends and associations. The researchers noted, "For example, a phone number with the 973 prefix/area code, associated with the state of New Jersey, was posted on 4 different sources and appeared in 55 listings."[2]

When analyzing the datasets, Insikt researchers found that many phone numbers and email addresses were present in posts from multiple sources, and many advertisements listed multiple locations for meetups. This gives insight into the collaborative and organized nature of the individuals and groups controlling the enterprise, and steps away from the misleading idea that these platforms are mainly used by individuals who are operating independently. In combination with the identified search terms, including "brothel", "buyer", "whore", "vic", and "purchase", Insikt researchers were able to develop a methodology for assisting law enforcement to identify the early warning signs and potential indicators of human trafficking. Utilizing OSINT tools, Insikt researchers found the same phone numbers and email addresses hundreds of times in posts across multiple sources, allowing them to find identifying information that could assist law enforcement to attribute this data to victims and/or actual traffickers.

Figure 2. Examples of key words from the same website

Researchers broke the methodology into three (3) phases: Identify, Triage, and Investigate. The first is "Identify and Collect Contact Information," which is the preliminary phase where investigators analyze human trafficking sources based on known trafficking keywords, collecting identifying artifacts like names, phone numbers, email addresses, and physical locations, as well as usernames and other online aliases. The second is "Triage Contact Information," where investigators sort through their list of contact information to identify trends and connections to other activity. The final phase is "Investigate," and this is the phase where investigators will utilize tools to identify additional information associated with an individual's contact information. This could include identifiers like owned domains, IP addresses, social media handles, or other email addresses attributed to the same individual or post. This evidence could support the probable cause needed to justify law enforcement in obtaining warrants and subpoenas to request user data from service providers like Google and AT&T, as well as social media companies like Meta.

Utilizing the power of the courts, law enforcement investigators can use the preliminary data that they've aggregated to obtain privileged user information such as sign-in IP addresses, SMS timestamps, or email message content from the service providers. This added granularity can enable investigators to place their suspects or victims in front of a specific internet-enabled device at the exact time that the suspected human trafficking data was generated, enabling the state to locate or charge and prosecute the individuals. With this PoC framework, Insikt Group researchers urged law enforcement agencies around the world to proactively look for and surface warning signs and potential indicators of human trafficking using the techniques described in the report. The continuous monitoring of adult classified sites known for sexual exploitation could also give law enforcement an edge, as many of these webpages do not timestamp their posts or listings as a way to evade the authorities. Daily data harvesting could give law enforcement insight into patterns and trends of traffickers, and email alerts and watchlists would help to establish accurate timelines.

The utilization of real-time threat-intelligence to monitor human sex trafficking activity has revolutionized how law enforcement agencies across the world tackle the problem. US organizations like the Anti-Human Trafficking Intelligence Initiative (ATII) and the Polk County Sheriff's Office Vice Unit in Florida ("Operation March Sadness 2") have both had great success enriching their investigations with threat-intelligence data to take down entire trafficking operations.[2] In September 2022, Europol organized a hackathon, utilizing law enforcement members from more than twenty (20) different countries monitoring 114 suspicious websites, leading to the identification of eleven (11) trafficking suspects and forty-five (45) possible victims.[3] With the internet now being the most-used vessel for traffickers to groom victims and coordinate their

[3] https://www.infosecurity-magazine.com/news/europol-hackathon-human/

operations, the use of data analytics will allow law enforcement to attack the problem at the source. Multiple traffickers who traditionally have been very hard for the authorities to attribute to the same operation can now be pinpointed by automated alerts, leading to far fewer leads going cold over time.

MONTI: SISTER ORGANIZATION OR IMPOSTER THREAT GROUP?

- Monti is an emerging threat organization who mimic TTPs of the Conti Ransomware Group.
- Monti ransomware attacks have been seen in the wild since July 2022, with rumored reports of activity in May 2022.
- Conti public data leak could be the backbone of the Monti threat group.

Summary

Over the past several weeks a new, potentially imposter, threat organization has mimicked the tactics, techniques, procedures (TTPs), and infrastructure of the Conti Ransomware Group. Tracked as MONTI, this doppelganger organization emerged in the threat landscape in July 2022 after compromising a company and encrypting approximately twenty (20) hosting devices and a multi-host VMWare ESXi instance tied to over twenty (20) additional servers. While the July attack pushed the group into the limelight, analysts believe that attacks from the doppelganger organization go back even further into the early summer of 2022.

According to security analysts at BlackBerry, previous attacks from the Monti threat group show exploitation of Log4Shell attack chain (CVE-2021-44228, CVE-2021-45046) on vulnerable VMWare Horizon instances.[4] After exploitation, attackers downloaded Google Chrome and began downloading payloads including Anydesk RMM (Remote Monitoring & Management) and Action1 RMM followed by Megasync, Putty, and WinSCP for data exfiltration and the ransomware encryption module.[5] With these tools combined, Monti threat actors possessed the capabilities to evaluate and remote into the victim's network, harvest account credentials, bypass anti-virus mechanisms, shift laterally throughout the network, encrypt devices and files, and exfiltrate data back to actor-controlled command-and-control (C2) servers.

Similarities discovered between Conti Ransomware and the alleged spinoff Monti Ransomware include attack TTPs alongside the reuse of Conti-attributed malicious payloads, deployed tools, and ransom notes. Additionally, the encrypted files exfiltrated by Monti contain a nearly identical encryption, which could indicate code reusage. However, back in February Conti's encryption source codes, 60,000 internal communication messages, and threat actor personal identifiable information was publicly leaked by a Ukrainian Conti threat actor due to opposing beliefs in the Ukraine/Russia geopolitical conflict.[6] While the code reusage in Monti ransomware attacks could indicate a rebrand, the public information leaked about Conti gives a group of threat actors the opportunity to mimic Conti TTPs, payloads, and tooling to carry out their own attacks.

[4] https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger
[5] https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger
[6] https://intel471.com/blog/conti-vs-monti-a-reinvention-or-just-a-simple-rebranding

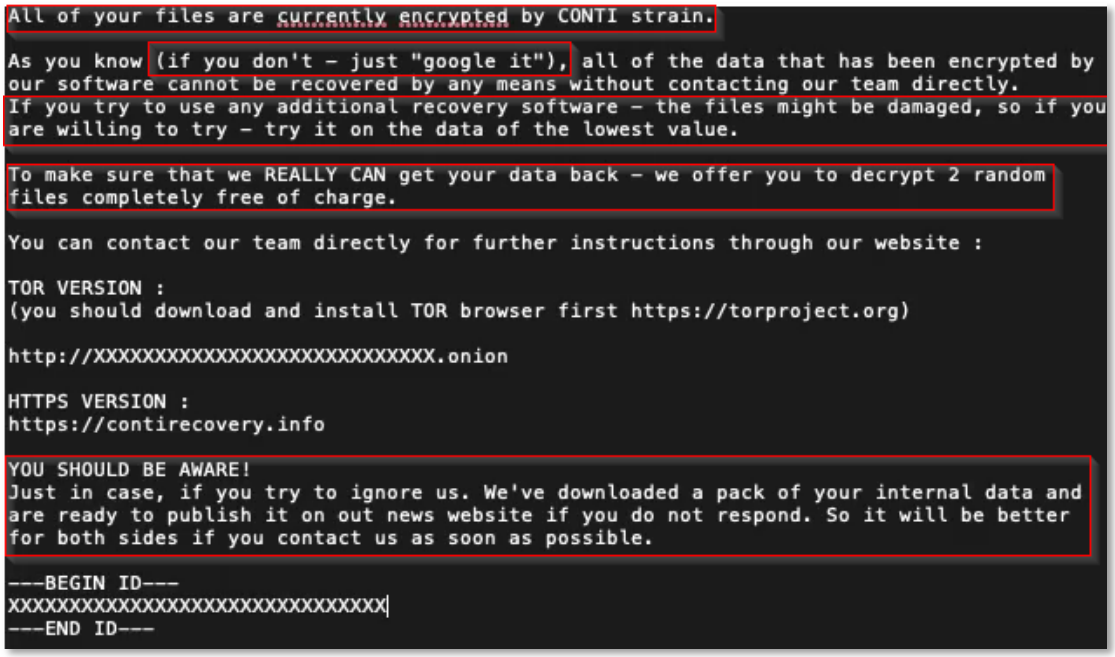

Figure 1: Conti Ransom Note

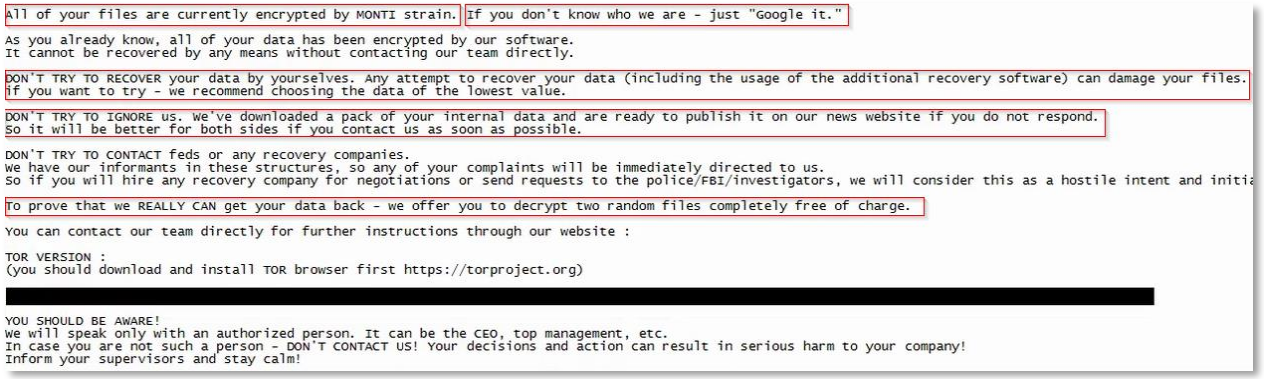

Figure 2: Monti Ransom Note

Since Monti is a lesser-known threat organization as of today, it is difficult to confirm whether Monti is a rebranding of Conti Ransomware or a new organization entirely. With a little less than a dozen rumored victims, Monti is just beginning to emerge into the ransomware scene. By utilizing TTPs disclosed by former Conti threat actors, this organization has equal, if not more, capabilities than the Conti Ransomware Group. In the coming months, CTIX analysts expect to see more movement from the Monti threat organization and an increased number of Conti-attributed IOCs connected to Monti ransomware attacks. CTIX will also continue to monitor threat actor activity worldwide and provide additional updates accordingly.

ANALYSIS OF IRANIAN STATE-SPONSORED THREAT ORGANIZATION'S ATTACK TIMELINE TARGETING THE ALBANIAN GOVERNMENT

- The Government of NATO-member Albania has been suffering cyber-attacks launched by Iranian state-sponsored threat organization "Homeland Justice" in July as well as September of 2022.
- Albanian is suspected to be the first country to sever diplomatic ties with another country due to a cyber-related attack.

Summary

In July 2022, nation-state Iranian threat actors, identified by the FBI as "Homeland Justice", launched a "destructive cyber-attack" against the Government of NATO-member Albania in which the group acquired initial access to the victim network approximately fourteen (14) months before (May of 2021).[7] During this period, the threat actors continuously accessed and exfiltrated email content. The peak activity was observed between May and June of 2022, where actors conducted lateral movements, network reconnaissance, and credential harvesting.[8] This attack and eventual data dumps were targeted against the Albania-based Iranian dissident group Mujahideen E-Khalq (MEK), otherwise known as People's Mojahedin Organization of Iran. MEK is a "controversial Iranian resistance group" that was exiled to Albania and once listed by the United States as a Foreign Terrorist Organization for activity in the 1970s but was later removed in late 2012.[9] Albania eventually severed diplomatic ties with Iran on September 7, 2022, and is suspected to be the first country to ever have done so due to cyber-related attacks.[10]

Activity first ramped up in June 2022, when the Iranian threat organization created a website and various social media profiles posting anti-MEK messages.[11] On July 17, 2022, "Homeland Justice" launched their destructive ransomware attack on the government's networks, which left an anti-MEK message on the machines and involved disk wiping malware, as well as soon after claimed responsibility for the destructive ransomware.[12] Microsoft researchers emphasized the timing of the cyber-attack against Albania, which occurred weeks after various cyberattacks on Iran, and was one (1) week ahead of the MEK-sponsored Free Iran World Summit.[13] The attack also "aligned with other Iranian policy moves against the MEK," noted the researchers.[14] A few days after the planned Free Iran World Summit, which was cancelled after the cyber-attack, Iranian official press issued an editorial "calling for military action against the MEK in Albania."[15] The researchers suspected that there may have been a "whole-of-government Iranian effort to counter the MEK from Iran's Ministry of Foreign Affairs, to intelligence agencies, to official press outlets."[16]

In late July, the threat organization posted videos of the cyberattack on their website and during that time until mid-August, the groups' social media accounts continuously advertised "Albanian Government information for release." During these advertisements, the group posted polls asking which government

---

[7] https://www.cisa.gov/uscert/ncas/alerts/aa22-264a
[8] https://www.cisa.gov/uscert/ncas/alerts/aa22-264a
[9] https://www.cfr.org/backgrounder/mujahadeen-e-khalq-mek
[10] https://www.washingtonpost.com/politics/2022/09/08/albania-is-first-known-country-sever-diplomatic-ties-over-cyberattack/
[11] https://www.cisa.gov/uscert/ncas/alerts/aa22-264a
[12] https://www.cisa.gov/uscert/ncas/alerts/aa22-264a
[13] https://www.microsoft.com/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/
[14] https://www.microsoft.com/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/
[15] https://www.microsoft.com/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/
[16] https://www.microsoft.com/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

information should be dumped, which later was released in either a ZIP file or through a video of a screen recording.[17] The actors shared internal government documents as well as Albanian residence permits, marriage certificates, passports, and images of MEK members. In September, "Homeland Justice" released a new wave of attacks with similar tactics, techniques, and procedures (TTPs) of those launched in July. It is speculated that this wave was conducted "in retaliation for public attribution of the cyber-attacks in July and severed diplomatic ties between Albania and Iran."[18]

Mandiant researchers published a comprehensive report[19] on August 4, 2022, that detailed the different malware observed in the attacks against the Government of Albania. The researchers identified "ROADSWEEP" and "CHIMNEYSWEEP" as malware used during the attack. ROADSWEEP is a newly discovered ransomware family that enumerates all files on an infected device and encrypts their content in blocks using Rivest Cipher 4 (RC4), a stream cipher that is widely used due to its simplicity and speed. A sample of the ransomware was submitted to a public malware repository from Albania on July 22, which, once executed, decrypted and dropped a "politically themed ransomware note suggesting it targeted the Albanian government."[20] The ransom note states, "Why should our taxes be spent on the benefit of DURRES terrorists?" Mandiant researchers also identified a Telegram persona of the same name that targets the Albanian government.

Figure 1: Homeland Justice Ransom Note Image[21]

CHIMNEYSWEEP, first identified in 2012, is a backdoor that uses Telegram or actor owned infrastructure as a command-and-control (C2) communication channel.[22] Interestingly, CHIMNEYSWEEP also shares code with the ROADSWEEP ransomware, and has been used to target Farsi and Arabic speakers in the

[17] https://www.cisa.gov/uscert/ncas/alerts/aa22-264a
[18] https://www.cisa.gov/uscert/ncas/alerts/aa22-264a
[19] https://www.mandiant.com/resources/blog/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against
[20] https://www.mandiant.com/resources/blog/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against
[21] https://www.mandiant.com/resources/blog/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against
[22] https://www.mandiant.com/resources/blog/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against

past. Like ROADSWEEP, CHIMNEYSWEEP uses an embedded RC4 key. The backdoor drops with a benign Word, Excel, or video file and a self-extracting archive with a legitimate digital certificate. In addition, the threat actors who have claimed responsibility for the attack also claim to have used a wiper malware as well. Currently, it is unclear as to which wiper was used, but Mandiant researchers identified that an Albanian user submitted a sample of the "ZEROCLEAR" wiper malware to a public malware repository on July 19, coinciding with the attack timeline. ZEROCLEAR has previously been reported to have links to Iranian threat actors.

On September 7, 2022, the White House released a statement[23] condemning Iran's cyberattack against Albania and on September 9, 2022, the United States Treasury Department's Office of Foreign Assets Control (OFAC) imposed sanctions on Iran's primary intelligence agency and its top official.[24] On September 21, 2022, the Federal Bureau of Investigations (FBI) and the Cybersecurity and Infrastructure Security Agency (CSA) released the joint advisory AA22-264A regarding the cyber operations against the Government of Albania in July and September of 2022, and attributed these attacks to Iranian state-sponsored threat actors.[25] The alert included a timeline of the observed activity and additional technical details about the infection chain, as well as files used by the threat actors during their attacks. The conflict between Iran and the Government of Albania is evolving and cyber-activity between the two (2) entities is expected to be ongoing. CTIX analysts will continue to monitor all movement from Iran as well as the "Homeland Justice" threat organization.

[23] https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/
[24] https://therecord.media/us-sanctions-iran-intelligence-agency-over-albania-cyberattack/
[25] https://www.cisa.gov/uscert/ncas/alerts/aa22-264a

BANNING RANSOMWARE PAYMENTS BECOMES HOT-BUTTON ISSUE IN STATE LEGISLATURE

- The ethics of allowing extorted businesses to negotiate and pay ransom demands on their own are being debated in US courts.
- Some states have already passed laws that prohibit extorted state agencies from paying ransoms.
- The evidence indicates that banning government entities from paying ransoms could make them less profitable to attack, potentially decreasing the number of ransomware incidents they face.

Summary

There is a debate occurring in courtrooms across the United States regarding the ethics and impacts of allowing businesses to make ransomware payments. North Carolina and Florida have broken new ground earlier this year passing laws that prohibit state agencies from paying cyber extortion ransom demands. In North Carolina's case, administrators and cybersecurity specialists assisting the organization are precluded from communicating with the threat actors. State agencies must also immediately report ransomware incidents to the North Carolina Department of Information Technology, allowing the North Carolina Joint Cybersecurity Task Force to gather data on and respond to these cyber events. Florida's ban on paying ransom demands followed just a few months after North Carolina's and requires reporting within twelve (12) hours of discovery. While these two (2) states have been leading the way in ransomware laws, at least twelve (12) other states have addressed ransomware in some way, adding criminal penalties for those involved and requiring public entities to report ransomware incidents.

There are many issues states have to negotiate when trying to pass ransomware legislature. One of the biggest hurdles lawmakers face is educating their fellow senators. New York State Senator Diane Savino attempted to craft a bill similar to the one's in Florida and North Carolina, though it never made it onto the Senate floor this year because, as Savino states, "quite obviously, [the other senators] don't understand it."[26] Savino also mentioned issues with the coordination and communication between the federal and state cybersecurity entities. Federal agencies simply do not provide much guidance to state and local governments when asked what course of action to take regarding ransomware and other cyber incidents.

According to the progress in states with new legislation like NC and FL, evidence indicates that government ransomware payment bans are a step in the right direction to curbing the ransomware threat. Ransomware groups survive on payments and continue to attack organizations because they know they will be rewarded for it. In theory, banning government entities from paying ransoms could make them less profitable to attack and potentially decreasing the number of ransomware incidents they face. While many are pushing for more states to enact these laws, some experts doubt their effectiveness. Brett Callow, a ransomware expert at Emsisoft, stated, "[Ransomware groups] understand that if they were to cease attacks in states with prohibitions, more states would introduce prohibitions. It is, therefore, in their best interests to continue attacking in states with bans." Allan Liska, a ransomware expert at Recorded Future, explained that he understands why lawmakers want to push these laws as they do not cost money and allow the politicians to gain favor with voters. The real fix, Liska suggests, is pouring more money into cybersecurity defense on a local level, stating "most small towns don't even have a full-time security person." Liska revealed another issue: if a government entity pays a ransom through a third-party, the threat groups can threaten the organization with releasing the details of the payment and demanding more money. While the debate on whether or not these laws help to curb ransomware attacks continues on, CTIX analysts will continue to monitor the situation and will provide updates for any new developments.

[26] https://therecord.media/an-inside-look-into-states-efforts-to-ban-govt-ransomware-payments/

THREAT ACTOR OF THE MONTH

- Worok has recently been discovered as a potential new cluster of TA428 as the group uses similar TTPs.
- TA428 is a Chinese advanced persistence threat (APT) group first identified in July 2019 during "Operation LagTime IT".

Summary

ESET researchers discovered a new cluster of the long-active TA428 identified as "Worok." TA428 is a Chinese advanced persistence threat (APT) group first identified by Proofpoint researchers in July 2019 during "Operation LagTime IT", a malicious attack campaign targeted against government IT agencies in East Asia.[27] The researchers discovered similarities to a surveillance operation conducted in 2013 through the payload and command-and-control (C2) infrastructure, indicating they may have been active for years before being attributed as a threat group.[28] In 2021, Recorded Future's Insikt Group identified more TA428 activity targeting Russian and Mongolian IT companies that overlapped with Operation LagTime IT.[29] TA428 additionally conducted "Operation StealthyTrident" in 2020, a Mongolian supply-chain attack discovered by Proofpoint in December of that year.[30] Most recently, TA428 has been detected by Kaspersky targeting military industrial organizations in Eastern Europe and Afghanistan at the start of 2022.[31]

Worok has recently been discovered by ESET researchers as a potential new cluster of TA428.[32] Worok uses similar tactics, techniques, and procedures (TTPs) as TA428, such as the use of the ShadowPad malware, activity times, and targeted verticals. Their objective is also to conduct cyber espionage across Asia. While the two (2) groups have similarities, they differ in other ways which leads to the distinction. In late 2020, Worok began targeting government entities and organizations in Asia, the Middle East, and Southern Africa. Shortly after their initial attacks, the group took a hiatus from mid-2021 to January 2022. Worok's initial access vectors are not well-known. The researchers were able to identify the use of the ProxyShell vulnerability (CVE-2021-34523) to gain initial access to Microsoft Exchange servers. Following initial access, the group deploys publicly available tools to perform reconnaissance. Worok has developed custom loaders to establish persistence on infected devices. Their original first-stage loader, dubbed "CLRLoad," is a Common Language Runtime (CLR) DLL file written in C++. CLRLoad was replaced by a fully featured PowerShell backdoor given the name "PowHeartBeat." This loader is hidden under two (2) layers of obfuscation to deter static analysis. PowHeartBeat communicates with its C2 server using HTTP or ICMP. It has the functionality to execute commands and processes, upload, download, and modify files, as well as gather information on the infected device. The PowHeartBeat loader then downloads and executes the second stage loader "PNGLoad." The second-stage loader uses PNG files and steganography, the technique of hiding data in images, to download and execute the final payload. The PNG files used by PNGLoad appear to be legitimate PNG files to hide in plain sight. Using these tools, they have been immensely successful in achieving their objectives. Worok is continuing to attack organizations and will likely continue to be a threat in the future.

[27] https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology
[28] https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2012/NormanShark-MaudiOperation.pdf
[29] https://www.recordedfuture.com/china-linked-ta428-threat-group
[30] https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/
[31] https://www.recordedfuture.com/china-linked-ta428-threat-group
[32] https://www.welivesecurity.com/2022/09/06/worok-big-picture/

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
b45fe91d2e2340939781d39daf606622e6d0b9ddacd8425cb8e49c56124c1d56	SHA256	Monti
158dcb26239a5db7a0eb67826178f1eaa0852d9d86e59afb86f04e88096a19bc	SHA256	Monti
702099b63cb2384e11f088d6bc33afbd43a4c91848f393581242a6a17f1b30a0	SHA256	Monti
9aa1f37517458d635eae4f9b43cb4770880ea0ee171e7e4ad155bbdee0cbe732	SHA256	Monti
df492b4cc7f644ad3e795155926d1fc8ece7327c0c5c8ea45561f24f5110ce54	SHA256	Monti
78517fb07ee5292da627c234b26b555413a459f8d7a9641e4a9fcc1099f06a3d	SHA256	Monti
81e123351eb80e605ad73268a5653ff3	MD5	Albanian Cyberattack - Error4.aspx: Webshell
7b71764236f244ae971742ee1bc6b098	MD5	Albanian Cyberattack - cl.exe: Wiper
bbe983dba3bf319621b447618548b740	MD5	Albanian Cyberattack - GoXML.exe: Encryptor
0738242a521bdfe1f3ecc173f1726aa1	MD5	Albanian Cyberattack-Goxml.jpg
a9fa6cfdba41c57d8094545e9b56db36	MD5	Albanian Cyberattack - ClientBin.aspx: Webshell (reverse-proxy connections)
8f766dea3afd410ebcd5df5994a3c571	MD5	Albanian Cyberattack - Pickers.aspx: Webshell
Unknown	MD5	Albanian Cyberattack - evaluatesiteupgrade.cs.aspx: Webshell
78562ba0069d4235f28efd01e3f32a82	MD5	Albanian Cyberattack - mellona.exe: Propagation for Encryptor
1635e1acd72809479e21b0ac5497a79b	MD5	Albanian Cyberattack - win.bat: Launches GoXml.exe on startup
18e01dee14167c1cf8a58b6a648ee049	MD5	Albanian Cyberattack - win.bat: Changes desktop background to encryption image
59a85e8ec23ef5b5c215cd5c8e5bc2ab	MD5	Albanian Cyberattack - bb.bat: Saves SAM and SYSTEM hives to C:\Temp, makes cab archive

60afb1e62ac61424a542b8c7b4d2cf01	MD5	Albanian Cyberattack - disable_defender.exe: Disables Windows Defender
8f6e7653807ebb57ecc549cef991d505	MD5	Albanian Cyberattack - rwdsk.sys: Raw disk driver utilized by wiper malware
e9b6ecbf0783fa9d6981bba76d949c94	MD5	Albanian Cyberattack - App_Web_bckwssht.dll
144[.]76[.]6[.]34	IP address	Albanian Cyberattack - Accessed web shell
148[.]251[.]232[.]252	IP address	Albanian Cyberattack - Accessed web shell
148[.]251[.]233[.]231	IP address	Albanian Cyberattack - Accessed web shell
176[.]9[.]18[.]143	IP address	Albanian Cyberattack - Accessed web shell
185[.]82[.]72[.]111	IP address	Albanian Cyberattack - Accessed web shell
216[.]24[.]219[.]65	IP address	Albanian Cyberattack - Accessed web shell
216[.]24[.]219[.]64	IP address	Albanian Cyberattack - Accessed web shell
46[.]30[.]189[.]66	IP address	Albanian Cyberattack - Accessed web shell
f116acc6508843f59e59fb5a8d643370dce82f492a217764521f46a856cc4cb5	SHA-256	Albanian Cyberattack - GoXml.exe
e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0	SHA-256	Albanian Cyberattack - “w.zip”, “cl.exe”, “cls5.exe”
bad65769c0b416bb16a82b5be11f1d4788239f8b2ba77ae57948b53a69e230a6	SHA-256	Albanian Cyberattack - Win.bat
bb45d8ffe245c361c04cca44d0df6e6bd7596cabd70070ffe0d9f519e3b620ea	SHA-256	Albanian Cyberattack - ADExplorer.exe
e67c7dbd51ba94ac4549cc9bcaabb97276e55aa20be9fae909f947b5b7691e6b	SHA-256	Albanian Cyberattack - Ldd.2.exe
ac4809764857a44b269b549f82d8d04c1294c420baa6b53e2f6b6cb4a3f7e9bd	SHA-256	Albanian Cyberattack - Mellona.exe
d1bec48c2a6a014d3708d210d48b68c545ac086f103016a20e862ac4a189279e	SHA-256	Albanian Cyberattack - Sl.exe
d145058398705d8e20468332162964dce5d9e2ad419f03b61adf64c7e6d26de5	SHA-256	Albanian Cyberattack - HxD.exe (Hex Editor)
1c926d4bf1a99b59391649f56abf9cd59548f5fcf6a0d923188e7e3cab1c95d0	SHA-256	Albanian Cyberattack - Lsdsk.exe
fb49dce92f9a028a1da3045f705a574f3c1997fe947e2c69699b17f07e5a552b	SHA-256	Albanian Cyberattack - NTDSAudit.exe
45bf0057b3121c6e444b316afafdd802d16083282d1cbfde3cdbf2a9d0915ace	SHA-256	Albanian Cyberattack - Disable-defender.exe
dfd631e4d1f94f7573861cf438f5a33fe8633238d8d51759d88658e4fbac160a	SHA-256	Albanian Cyberattack - Rognar.exe