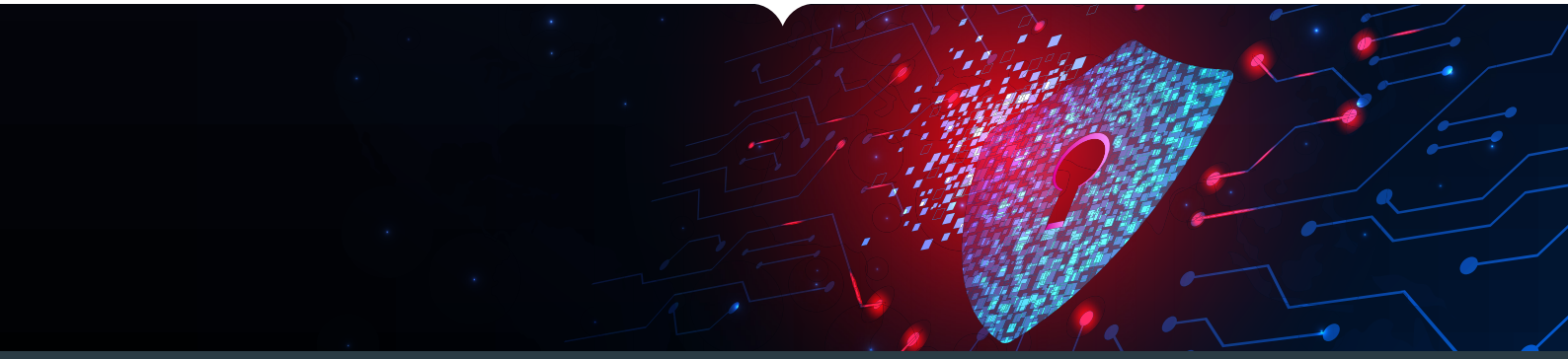
TRAVELERS



TRAVELERS BULLETIN Q1 2022

Ukraine targeted by cyber-attacks as Russian invasion continues

Government and banking websites in Ukraine were taken offline by a series of coordinated Distributed Denial of Service Attacks (DDoS), prior to the Russian invasion. Some compromised websites displayed anti-Ukraine messages, which warned citizens to "be afraid and prepared for the worst".

In the wake of the invasion, Western cybersecurity agencies have been on high alert fearing Russian retaliation for sanctions that are crippling its economy. The UK's National Cyber Security Centre has advised organisations to exercise additional diligence in ensuring their systems are secure and their staff use strong and unique passwords.

Russia's invasion of Ukraine has undoubtably elevated the security risk posed by cyber-attacks. Organisations in countries considered unfriendly by Russia are firmly in the crosshairs of the country's offensive cyber capabilities. Organisations should review their cybersecurity policies and contingency plans.

New types of malware were discovered to have been used against Ukraine. A new trojan dubbed as "FoxBlade" allows attackers to use compromised computers to conduct DDoS attacks. Several new varieties of disk-wiping malware, such as "Whispergate" and "HermeticWiper", have also been used against Ukraine to destroy data and render systems inoperable.

Organisations should remember that data backups are an essential part of reducing the impact of data-wiping and ransomware cyber-attacks.

New malware and vulnerabilities used in the conflict could be reused by criminal actors for financial gain, putting everyone at risk. Keeping IT systems up to date with the latest software patches is the best line of defence against new attack methods.

Russia has allegedly targeted Ukraine's critical infrastructure with its offensive cyber capabilities in the past, but has yet to do so since the conflict began. A cyber-attack on Ukraine's power grid in 2015 resulted in 230,000 consumers being left without power for up to six hours. Analysts believe there is potential for more devastating cyber-attacks to be carried out against Ukraine in the near future.

Cyber-attacks originating from Russia have the potential to increase as economic deprivation pushes more towards cybercrime. The private sector continues to be a lucrative target for ransomware attacks and data theft. Organisations can mitigate these attacks by ensuring employees are able to spot phishing attempts, which often enable these attacks.

Useful Resources

- https://www.reuters.com/world/europe/ukrainian-government-foreign-ministry-parliament-websites-down-2022-02-23
- https://www.zdnet.com/article/ukrainian-govt-sites-banks-disrupted-by-ddos-amid-invasion-fears/
- https://www.cisa.gov/uscert/ncas/alerts/aa22-057a
- https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
- https://threatpost.com/microsoft-ukraine-foxblade-trojan-hours-before-russian-invasion/178702/
- https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened

Red Cross data exposed using unpatched ManageEngine flaw

The International Committee of the Red Cross (ICRC), a world-renowned humanitarian organisation, has had personal data belonging to over half a million "highly vulnerable people" potentially stolen from its servers. The attack was reportedly facilitated by an unpatched vulnerability in a password management and single sign-on (SSO) platform called "Zoho ManageEngine ADSelfService Plus."

The ICRC discovered their servers had been compromised on 18 January 2022 and believes they were hacked on 9 November 2021. Attackers had a 70-day window to access the ICRC's data. The data itself was reportedly encrypted but contained highly sensitive personal information about individuals who were receiving assistance from the organisation, which specialises in helping those affected by armed conflict and natural disasters.

Data theft that potentially exposes personal information of individuals puts the victim organisation at a high risk of costly litigation. Organisations should handle personal data according to guidance set out by the data protection agency of their jurisdiction and familiarise themselves with their data breach reporting obligations.

The vulnerability, CVE-2021-40539, was patched on 7 September 2021 by the software manufacturer Zoho after being discovered in August. CVE-2021-40539 allows an attacker to bypass authentication measures, which can allow them to execute malicious code remotely. The vulnerability affects ADSelfService Plus up to build 6113, and the manufacturer is advising customers to install the latest build immediately.

Keeping systems up to date is one of the best ways to prevent cyber-attacks. Organisations should routinely check and implement software patches and fixes, particularly ones listed as critical by the manufacturer.

The ICRC has said it could not ascertain who orchestrated the attack against its systems or what motivated the attack. No actor has come forward to claim the hack or ask for a ransom. The organisation does not currently believe that its data has been published online or sold.

Useful Resources

- https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know
- https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html
- https://www.paloaltonetworks.com/blog/security-operations/zoho-manageengine-adselfservice-plus-cve-2021-40539/
- https://portswigger.net/daily-swig/red-cross-servers-were-hacked-via-unpatched-manageengine-flaw

Conti Ransomware Group data leak

The Conti Ransomware Group has quickly gained notoriety in just a couple of years, becoming one of the most successful and ruthless cyber-criminal groups the world has seen. The group generated a reported $180 million in revenue in the last year, after several high-profile attacks against very large organisations. They have also become well-known for their financial motivation over everything else. In the past, we have seen groups such as Anonymous setting out ethical rules for their hacks, targeting companies and organisations which go against their beliefs. Conti, however, operate with no moral compass, notably acting out a wave of cyber-attacks on over 400 hospitals in the US and UK at the height of the Covid-19 pandemic.

On 27 February 2022, a Ukrainian member of the Conti Ransomware Group began leaking internal data after the group had put out a message of support for the Russian Government a few days beforehand. The leaked data included the source code of the ransomware, Crypto Wallet addresses, internal chat logs, usernames, passwords, and other sensitive data which was taken from the group's Jabber server. An internal leak of this scale from a ransomware group has never been seen before, and some cybersecurity professionals are referring to this case as the "Panama Papers of Ransomware".

Within this leak, there are also clear links between the Russian State and the group, with conversations surrounding the Bellingcat investigative journalism group. In the translated conversations, it appears the Conti hackers are searching Bellingcat's network (the company Alexei Navalny used to help identify his would-be killers) on behalf of someone else. For example, "Okay, look for stuff that's related to Navalny" and "Okay, save this stuff related to Navalny and save it in the folder Navalny FSB". Whilst this does not necessarily mean that the hackers were acting under the explicit command of the FSB (Russia's internal security and counter-intelligence agency), it does suggest that there may be some sort of relationship with the Russian State. This may also explain the statement in support of Russia at the beginning of the invasion of Ukraine.

It is worth noting that although this leak is invaluable to cybersecurity professionals and researchers, providing an opportunity to see all the inner workings of one of the most prolific ransomware groups, it may also give less experienced cyber criminals

an in-depth look at the source code of the ransomware, which they can then adapt and use for themselves. Although it appears that larger criminal groups like Conti and Anonymous are distracted by the Ukrainian war, XCyber® Group believes that in the following months, we will see other groups adopting parts of Conti's techniques and code in an attempt to profit for themselves.

US President Joe Biden recently issued a warning to US-based companies around the increased threat of cyber-attacks. For the time being, this may deter other threat actors who are thinking about using parts of the Conti Ransomware, due to the heightened attention and increased risk of conducting a cyber-attack. XCyber® Group believe that this may deter threat actors from targeting US-based companies. However, the warning could also encourage hackers to move to target international companies which are not US-based or involved in the Ukrainian conflict, as this warning indicates that the attention from authorities is likely to be focused elsewhere.

Useful Resources

- https://therecord.media/conti-leaks-the-panama-papers-of-ransomware

Lapsus$ Ransomware group

In recent months, the Lapsus$ Ransomware group has become one of the most prolific cyber-criminal organisations on the Internet. They have been credited for a number of high-profile attacks against companies like Nvidia, Microsoft, Okta and Samsung – all of which have occurred in the first quarter of 2022. The group first originated at the turn of the year, when they announced that they had stolen data from the Portuguese media company, Impresa. Since then, Lapsus$ have been relentless in targeting large organisations, gaining attention which has propelled them to the forefront of the ransomware world.

However, this attention was not all beneficial for the members. On 25 March 2022, the BBC released an article stating that a 16-year-old boy from Oxford had been arrested after being suspected of being one of the leaders of the Lapsus$ group. The article went on further to state that an additional six people aged between 16 and 21 had been arrested in the UK, with links to the gang. The teen, known as 'White' or 'Breachbase', allegedly made over $14 million from hacking which was disclosed – likely by former estranged business partners – within a doxing document, which reveals identifying information about an individual online. The 16-year old's name, address, social media accounts and photos were announced within the document.

The cybersecurity research company, Unit 221B, stated that they had been tracking White for over a year after linking him to several hacking incidents throughout 2021. Allison Nixon, the chief research officer at Unit 221B, claimed they were able to confidently link the teen to the attacks due to a trail of activity on the boy's online accounts. By trawling through the post history of the accounts, they were able to identify contact information for the boy. This was all passed on to law enforcement who had also periodically received updates about White's activities, all the way up until his arrest.

The Lapsus$ group differs from many of other ransomware groups; they are not afraid of the risks, often openly bragging about the names of the organisations they have breached. The group also operates in a different way to the typical exfiltrate-encrypt-extort method used by the vast majority of ransomware groups. Instead, they opt to gain access to systems using phishing attacks and steal the most sensitive data without using data encryption malware. These actions, as well as doing things like redirecting top-level domains of victims to adult video sites, indicates that the group is very capable, but perhaps young or inexperienced.

The Covid-19 pandemic has caused more people to be inside and in front of their phones and computers than ever before. We have seen an uptick in almost everything technology-related in this time, such as social media, remote working apps such as Zoom and Microsoft Teams, and online education tools. It is logical that we are beginning to see these types of younger hackers and cybercriminals becoming more prominent, as people have never been trapped in their house for so long with little to do.

XCyber® Group believes that in the following months and years, we will see more cybercriminal groups adopting the Lapsus$ group's methodology. We will continue to see the usual political, social, and financial motivation behind cyber-attacks, but we believe we will also begin to see groups, especially younger ones, becoming more interested in creating havoc, having fun, and making a name for themselves as bigger motivations behind their attacks

Useful Resources

- https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/
- https://www.bbc.co.uk/news/technology-60864283
- https://thecyberwire.com/newsletters/privacy-briefing/4/52

Russian cyberattacks on Ukraine utilising Western infrastructure

According to Dutch news service NRC, a Russia-attributed botnet that was allegedly responsible for attacking the Ukrainian banking system was being controlled from a computer server in the North Holland village of Wormer.

The owners of the hosting company that provided the server are reportedly already under criminal investigation, as their customers are alleged to allow the proliferation of child pornography, spam bots, illegal drugs trading, and copyright violation.

A spokesperson for the company was said to have taken the server offline following contact from the Dutch authorities.

Likewise, further analysis of technical reports on a Russian state-backed hacker group known as "Sandworm" reveals their "Cyclops Blink" computer attacks are being conducted using servers in Italy, France, Germany, and the US on infrastructure managed by companies such as Vodafone, Comcast, Orange, and Deutsche Telekom.

Whilst there is no suggestion that any of these companies are complicit in the attacks, it highlights the potential for bad actors to abuse and misuse Western systems to damage Western interests – often undetected, and often with impunity.

The UK's National Cyber Security Centre, along with several US agencies including the NSA, have identified that the actor known as "Sandworm" or "Voodoo Bear" is attributed to the Russian GRU's Main Centre for Special Technologies GTsST.

The GRU's GTsST have previously been linked to:

- The BlackEnergy disruption of Ukrainian electricity in 2015
- Industroyer in 2016
- NotPetya in 2017
- Attacks against the Winter Olympics and Paralympics in 2018
- A series of disruptive attacks against Georgia in 2019

Meanwhile, as the cyber-attacks continue, rendering several official websites offline, the State Emergency Service of Ukraine has turned to Western social media websites such as Facebook to publish updates for Ukrainian citizens, sharing images and videos of the impact of shelling alongside guidance on what to do when hearing emergency alerts.

Useful Resources

- https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine
- https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf
- https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter

About Us

Solve commercial problems with state-grade intelligence expertise. We are a bespoke cyber intelligence company with extensive experience in producing actionable intelligence for our clients. Our team are pioneers in cyber and the company draws its talent from former members of the UK's Public Sector, who bring with them many years of **outcome-driven, operational cyber experience** and specialised skills working across numerous Government departments and the UK's Intelligence and Security Agencies.

We focus on producing **intelligence-led, data-driven** and **evidence-based** reporting which enables decision making across our clients' varying needs. All our intelligence is delivered in qualitative, narrative format, providing actionable information that is easy to digest.

Our clients rely on our ability to do **scalable technical work**, translate that into human-readable analysis and actionable leads, all while maintaining a team culture that - in partnership with our clients - increases value through its **candour** and **integrity**.

Our modus operandum is to be a **strategic consultative partner**, led by a team of some of the most experienced professionals in cyber intelligence across the entire world. Together they have been working to develop and deliver effective solutions to some of the most **complex and challenging cyber** problems faced in both the public and private sectors.

Our current portfolio of client intelligence requirements includes the following thematic areas, across multiple geographic regions and sectors:

- Internal investigations (including insider threat), counter-intelligence, and specialist research (including counter terrorism, unlawful activism, and election integrity).
- Online reputation and defamation investigations, intellectual property and brand infringement (including counterfeiting and responding to disinformation campaigns).
- Countering cyber-enabled fraud and criminality (investigating and lawfully disabling the criminal ecosystems).
- Cyber risk and advisory at strategic, operational and tactical levels - including data protection, privacy and security.
- Supplier and supply-chain assurance, competitor analysis, crisis and breach response, red-teaming, and personal risk reports for executives.

To learn more about how **XCyber®** can support your business and clients, please contact our London, Mayfair office on the following address:

enquiries@xcybergroup.com

Our operational requirements team will be pleased to meet you.

xcyber®

THE HUMAN SIDE OF CYBER®

If you have found this useful and would like to receive these quarterly updates direct to your inbox please **click here** to register