Waterstons
we're with you

+44 345 094 0945
www.waterstons.com

News article

Dec 2023

Cyber Attack News

Key cyber attack news from around the globe.

In an era defined by technological interconnectivity, our team at Waterstons is at the forefront of monitoring and reporting on key cyber incidents worldwide. As dedicated experts in the cybersecurity domain, we meticulously curate essential news to provide you, our valued clients, with insights into the ever-evolving digital landscape.

From high-profile breaches to emerging threats, our concise cyber incident review delivers strategic analyses and actionable recommendations, empowering you to navigate the complexities of the digital frontier with confidence. Join us in staying ahead of cyber challenges, as we bring you a succinct yet comprehensive overview of the critical events shaping our interconnected world.

USB worm unleashed by Russian hackers spreads worldwide

A USB worm created by Russian affiliated state sponsored threat actors targeting Ukrainian organisations, has spread outside of Ukraine and been observed in organisations across the world.

What Happened?

Over the past few months, the Gamaredon threat group has been almost exclusively targeting Ukrainian organisations, with the primary aim of exfiltrating sensitive data. One of the recent campaigns has involved a computer worm which spreads via removable media devices. Once a machine is infected, the worm will attempt to infect other connected USB devices to spread further, as well as download malware to enable data exfiltration. While the majority of injections occurred in Ukraine, security researchers have observed that the USB worm also appears to have been identified in organisations in the USA, Germany, Poland, Vietnam, Chile, and Hong Kong.

Researchers have been able to track the spread of the worm by observing uploads to VirusTotal, a website used by organisations that identify suspicious files on networks and want to find out if they are malicious. Currently there have been no reports of data breaches outside of Ukraine caused by this campaign, although it continues to spread across the world. Wider Implications

This incident highlights the 'spill over risk' of state sponsored cyber attacks that can impact organisations not typically a target of these threat actors. This incident is reminiscent of previous cyber attacks on Ukraine by Russia affiliated threat actors which also spread beyond the targeted organisations, such as NotPetya in 2017 which infected organisations across Europe and the USA.

This incident also highlights the enduring threat of removable media. Despite the significant cyber security risks associated with removable media and the widespread adoption of alternative solutions such as cloud storage and sharing solutions, USB sticks are still used by many organisations. Whilst it is currently unknown exactly how the USB worm, named LitterDrifter, has spread beyond the initial targets in Ukraine, it demonstrates how widespread USB storage device usage is and how it can still be an effective way of unwittingly transmitting malware between organisations and countries.

Organisations Should

• Organisations that would not typically be targeted by state sponsored threat actors should remain aware of the growing cyber threat from nation states and ensure that they continue to follow a cyber security strategy to address key risks. Organisations should focus on addressing the most common security misconfigurations identified by CISA: the use of default configurations of software and applications, improper separation of user/administrator privilege, insufficient internal network monitoring, lack of network segmentation, and poor patch management. Full report from CISA is available here.

• Review the use of removable media and restrict its usage where achievable – with the prevalence of cloud storage and sharing, organisations should prevent the use of USB devices unless there is no alternative solution.

• Ensure that where USB devices are required for business operations, they are procured by the organisation, rather than relying on employees' personal USB's. Any removable media should be scanned prior to being used on company devices, and encryption used wherever possible.

Russian FSB cyber actor Star Blizzard continues worldwide spear-phishing campaigns

The UK NCSC and international partners have issued a warning about a Russia based threat actor Star Blizzard, which has been observed carrying out a prolonged spear phishing campaign targeting organisations primarily in the UK and USA.

What Happened

The Russia based Star Blizzard threat actor group has been observed carrying out spear phishing campaigns targeting UK and US organisations, as well as organisations in other NATO countries, since 2019. These attacks have primarily targeted the education sector, defence, non-governmental organisations (NGO), think tanks, politicians, government bodies, and more recently the energy sector.

Anatomy of The Attack

The attacks start with significant research on the target. This can involve reconnaissance on targets' professional and personal social media to understand their interests to help craft the social engineering attack. The threat actor will then create fake email accounts impersonating the targets' contacts, as well as fake social media accounts to infiltrate the professional network. In some cases, they will use fake conferences or organisations, creating websites to convince targets of their legitimacy. Unlike many phishing attacks, Star Blizzard will typically target users' personal email addresses to avoid the security controls on enterprise email.

Typically, users will also be less vigilant of phishing emails when checking personal email, making it a more effective route for initial contact and deployment of malware – especially if users check personal email on work devices or vice versa. Once the threat actor has established contact with the target, they will typically spend an extended period of time establishing regular correspondence and building trust.

This patient approach is different to many phishing attacks, but can be far more effective. Once trust is established the threat actor will send a link directing the target to a malicious sign-in page to harvest their credentials. Star Blizzard also use EvilGinx to launch a Man in the Middle (MIM) attack to capture session cookies when a user logs in, allowing them to bypass MFA. Once they have access to an email account, the threat actor will setup mail forwarding rules to maintain persistent access even after the credentials are reset.

Organisations Should

• Evaluate their own risk profile to determine if they could be targeted by this or similar campaigns, using Star Blizzard's targeting profile as a guide, which is outlined in the advisory from the UK NCSC.

• Ensure that they are monitoring for the creation of any suspicious email forwarding rules since this may be an indicator of compromise (IoC). Any account that the organisation believes has been compromised should be investigated to identify any email forwarding rules were created.

• Implement conditional access controls such as impossible travel and geolocation to reduce the risk of a threat actor using compromised credentials and session cookies to bypass MFA and access an account. Where possible a VPN should also be required to access organisation systems.

• Ensure that high profile users at the organisation are provided with enhanced cyber security training to ensure they are aware of the sophisticated cyber threats that they may face both in and outside of work. This should also include a warning to be mindful of what information they post publicly since this could be used to craft targeted phishing attacks.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430