Waterstons
we’re with you

+44 345 094 0945
www.waterstons.com

Article

Mar 2024

February Cyber Attack News

Security researchers have identified an ongoing spear-phishing campaign targeting – and successfully compromising - Azure accounts belonging to senior leadership employees in dozens of organisations.

Spear-phishing campaign observed targeting senior leadership

Security researchers have identified an ongoing spear-phishing campaign targeting – and successfully compromising - Azure accounts belonging to senior leadership employees in dozens of organisations. **New Extortion Tactics** Since November 2023, security researchers have been tracking a spear-phishing campaign which has primarily targeted senior employees within organisations, up to and including the CEO.

The campaign delivers malicious phishing links embedded within documents shared via email and, when the target opens the document, they are redirected to a malicious login page to steal their Azure credentials.

Once they have obtained the account credentials, the threat actors will register their own MFA to establish persistent access to the account, before exfiltrating sensitive data. The attackers will then send further phishing emails from the compromised account both to internal and external recipients, some of which aim to compromise further accounts with others targeting internal departments (such as finance) to convince them to send money to the threat actors. The threat actors will also create mailbox rules to help hide evidence of the account compromise.

So far, the campaign has successfully compromised hundreds of Azure accounts belonging to senior leadership across dozens of organisations. As the campaign continues to operate organisations, should be wary of this ongoing targeted threat.

Wider Implications

Phishing attacks are an ever-present threat to organisations, being the initial infiltration vector in 41% of incidents according to the 2023 ENISA threat report. While generic phishing attacks are far more common, spear-phishing emails tailored to the target have a far higher success rate. For senior leadership at organisations, this threat can be increased due to the often-larger amount of publicly available information about them, allowing phishing emails to be targeted more effectively. Despite this increased effectiveness of spear-phishing emails, standard email security measures are just as effective at stopping them.

Organisations Should

- Ensure they have implemented number matching MFA on all accounts to reduce the risk of account compromises. This should be supported by additional conditional access controls such as geolocation restrictions, trusted devices, and blocking risk sign-ins.
- Consider advanced email security and web filtering solutions to significantly reduce the risk of phishing with more advanced social engineering threats, by blocking them before they reach end users.
- Ensure employees receive regular awareness training on the common types of threats they will face and how to identify them. Organisations should also ensure senior leadership receive regular, focused awareness training on the targeted types of threats they may face.

CISA releases report on the state-sponsored attacks on US CNI

The US Cybersecurity and Infrastructure Security Agency has released a report with international partners detailing the tactics used by Volt Typhoon in attacks on US Critical National Infrastructure (CNI), which has gone undetected in some organisations for up to five years.

Volt Typhoon Tactics and Techniques

The report follows an extensive investigation by CISA and their international partners, including the UK National Cyber Security Centre (NCSC) and the Australian Cyber Security Centre (ACSC), into state sponsored cyber-attacks on US CNI.

The report is centred on the Volt Typhoon threat actor which has been observed targeting a range of CNI organisations in the US, including communications, energy, transportation, water, and wastewater systems organisations. Unlike many threat actors, Volt Typhoon only extracts limited amounts of data to gather intelligence and appears to have focused on obtaining persistence within the organisation's environment. CISA has concluded that the aim of the threat actor is to establish widespread access within US CNI, in the 'event of a major crisis or conflict with the United States'.

While this report is into the specific tactics of one state-sponsored threat actor operating primarily in the US, the lessons learned in these attacks will be applicable to CNI organisations across the world. The report highlights the tactics used by Volt Typhoon in its attacks, with some of the most important summarised below. Visit here for the full report.

Initial infiltration

The primary method of initial infiltration that Volt Typhoon has been observed using against CNI, is the exploitation of vulnerabilities in public facing services. Prior to carrying out an attack, Volt Typhoon will conduct extensive reconnaissance both on staff and the organisation's publicly facing infrastructure. In particular, Volt Typhoon has been observed targeting network devices, including VPN's, Firewalls, and routers. While some of these vulnerabilities were zero-days, some were publicly known vulnerabilities with a patch available, that had not been applied by the targeted organisations.

Privilege Escalation

Once the threat actor has obtained access to the target organisation's network, they quickly look to obtain privileged access within the environment. The primary method of privilege escalation is the exploitation of internal vulnerabilities in Operating Systems (OS) or network services. They have also been observed searching for and obtaining credentials which have been stored in an unencrypted and insecure location such as a publicly facing network appliance.

Using privileged access, Volt Typhoon will typically try and laterally move to the OT network in order to begin exfiltrating sensitive data on the OT equipment, such as Supervisory Control and Data Acquisition (SCADA) systems, relays, and switchgear.

Establishing Persistence

In order to establish persistence, the threat actors will look to compromise additional accounts. To do this they will use a compromised domain administrator account to target the Ntds.dit file on the Domain Controller (DC). This file contains the AD database, including usernames, hashed passwords, and group membership for all accounts on the domain. They will then exfiltrate this file and attempt to crack the passwords offline. Based on suspicious activity from some accounts in the targeted organisations, the threat actors were able to crack the passwords of some accounts.

In some instances where Volt Typhoon has remained in the network for several years, they have been observed repeatedly exfiltrating the Ntds.dit file to obtain the latest account details.

In order to evade detection software, Volt Typhoon will often conduct an attack over a long period of time to avoid generating a significant number of logs that would trigger an alert. In some cases, they have been active on an organisation's network for five years before being identified.

Data Exfiltration

Once administrative access has been obtained, Volt Typhoon will typically target OT network diagrams and device configuration documents. It appears that the attacks were primarily interested in data gathering about the Industrial Control Systems (ICS) in place, potentially to help craft targeted attacks for the future that would have a physical impact.

Organisations Should

- Implement a patch management policy/process, setting clear governance rules for ensuring all software and firmware is kept up to date. This will reduce the risk of previously announced vulnerabilities offering an easy route for attackers into an organisation's network. This should be further underpinned by establishing a reporting mechanism to identify the age, severity and quantity of live vulnerabilities within the network. Such criteria can allow an organisation to assess the effectiveness of its patch management system.
- Ensure the patch management policy is supported by auto patch management solutions which can automatically keep some servers, endpoints and applications up to date.
- Implement a vulnerability management process that uses a risk-based process to prioritise the remediation of emerging vulnerabilities. With threat actors increasingly exploiting emerging vulnerabilities, organisations must reduce their 'time to patch'. This is especially important for zero-day vulnerabilities, which are already under active exploit, requiring organisations to deploy patches as soon as they are available.
- Adopt network segmentation, using well established models such as the Purdue model, which divides the enterprise network into six layers. This can help to contain threats cyber threats that infect and IT/OT network, as well as enable more effective business continuity plans, by enabling portions of the network to be taken down independently if required. This secure architecture should also consider what remote access to OT infrastructure is required and how this can be achieved securely.
- Ensure that they have implemented a process to manage Operating Systems (OS) for legacy versions to ensure upgrades are completed in plenty of time.
- Implement defence in depth security measures to ensure they do not rely on only one security control, especially where the risk of legacy systems must be accepted, even temporarily, for operational reasons. This should include controls such as isolating the legacy asset from the network through the use of VLAN.
- Ensure they have implemented a cyber detection strategy that has visibility on all endpoints, servers, and cloud solutions to ensure any malicious activity is detected quickly. CNI organisations should ensure that any detection tooling is also designed to operate in OT environments to ensure the organisations full infrastructure is monitored. This detection software should be monitored 24/7 to ensure any malicious activity is investigated immediately.
- Ensure that file integrity changes are monitored as part of the cyber detection strategy, to ensure that suspicious activity in key system files is identified and contained quickly.
- Ensure that conditional access controls are applied for accounts, such as risky sign ins and impossible travel. This will help identify and block compromised accounts.

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 I 02 9160 8430