Strategic Cyber Security Report for Leaders— September 2022 Edition

A Monthly summary of Strategic Information for Cyber Security Leaders

This is a series spun from a need I identified when talking to CISOs — as explained on the kick-off article, this series follows the format of:

CISO's Top of mind in 3 domains: People, Processes and Technology.

People

Keeping the team up with how to best utilize their Toolset

- Microsoft Defender for Office 365 — SecOps Guide

Late in September, Microsoft released the Microsoft Defender for Office 365 Security Operations Guide (SecOps).

SecOps needs to onboard the new tools and tasks into their existing playbooks and workflows. We often hear this presents a challenge for teams and raises questions, such as: "Where do I start? What actions/tasks should I take? How do I integrate with my existing tools and processes?"

The Microsoft Defender for Office 365 Security Operations Guide provides useful information to answer the above questions.

Here's the link to the guide, a great resource for cybersecurity teams using this tool.

And just as important as operating the platform is knowing how to handle its incidents from the XDR dashboard, M365 Defender. And for this purpose, access this guide.

- Configuration guides for Australian Government Essential 8

Microsoft released a number of Best practice configuration guides to help organizations adhere to Essential 8.

All are public and available here.

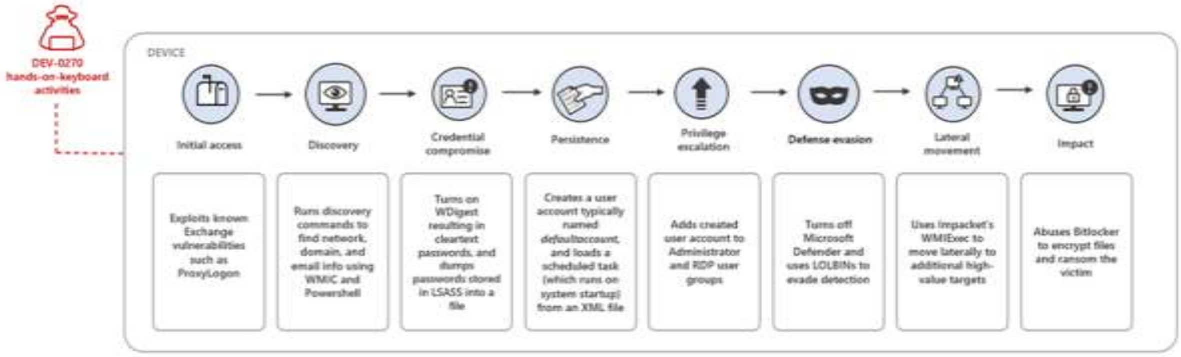
Strategic Information on Research around Major threat actors

- Phosphorous Ransomware operation

Source, Microsoft Threat Intelligence

Microsoft threat intelligence teams have been tracking multiple ransomware campaigns and have tied these attacks to DEV-0270, also known as Nemesis Kitten, a sub-group of Iranian actor PHOSPHORUS. Microsoft assesses with moderate *confidence that DEV-0270 conducts malicious network operations, including widespread vulnerability scanning, on behalf of the government of Iran.*

A typical attach chain for this operator:


DEV-0270
hands-on-keyboard activities
DEVICE
Initial access
Discovery
Credential compromise
Persistence
Privilege escalation
Defense evasion
Lateral movement
Impact
Exploits known Exchange vulnerabilities such as ProxyLogon
Runs discovery commands to find network, domain, and email info using WMIC and Powershell
Turns on WDigest resulting in cleartext passwords, and dumps passwords stored in LSASS into a file
Creates a user account typically named defaultaccount, and loads a scheduled task (which runs on system startup) from an XML file
Adds created user account to Administrator and RDP user groups
Turns off Microsoft Defender and uses LOLBINs to evade detection
Uses Impacket's WMIExec to move laterally to additional high-value targets
Abuses Bitlocker to encrypt files and ransom the victim

Observed techniques and recommendations to curb their actions and KQL queries for your team to run are highlighted in the original report.

And remember you can look for major threats in your environment with **Microsoft's XDR using Threat Analytics** which saves cyber security analysts hunting time amongst other benefits… Learn more about it here and in this video.

- Mid-year threat reports

Vendors have started making available their threat reports for the mid-year. One of them is Trend Micro — report and info in their official website here.

Process

NZ Information Security Manual Updates

Earlier this month the NZ ISM received an update. With release v3.6 a few policy changes were made to it. A summary of the changes were provided by GCSB:

“Updates finalised for the v3.6 release of the NZISM include four policy changes (a new chapter on Public Cloud Security, a new section on Inverse Split-tunnel VPN, language modernisation throughout the NZISM and updates to DMARC/DKIM in section 15.2) and a small number of minor and editorial changes.
These changes are driven by system threats and risks identified through enquiries from agencies, our own research, information security policy gaps highlighted by changes in the way government agencies now use cloud technologies, and changes to the international security frameworks and standards that the NZISM is based on. We also continue to engage with international partners and develop our policy and standards in line with theirs.”

Have a look at all details here.

Technology

- Uber suffers major attack

Uber suffered a cyber-attack this month, it made the announcement and provided some investigation updates through an official post, below.

Source, Uber:

An Uber EXT contractor had their account compromised by an attacker. It is likely that the attacker purchased the contractor’s Uber corporate password on the dark web, after the contractor’s personal device had been infected with malware, exposing those credentials. The attacker then repeatedly tried to log in to the contractor’s Uber account. Each time, the contractor received a two-factor login approval request, which initially blocked access. Eventually, however, the contractor accepted one, and the attacker successfully logged in.

From there, the attacker accessed several other employee accounts which ultimately gave the attacker elevated permissions to a number of tools, including G-Suite and Slack. The attacker then posted a message to a company-wide Slack channel, which many of you saw, and reconfigured Uber's OpenDNS to display a graphic image to employees on some internal sites.

The responsible was identified and arrested a few days later, a 17-year-old from London was blamed for this incident and apparently also responsible for hacking Rockstar and leaking GTA 6 footage, source hackernews.

Both the intrusions are alleged to have been committed by the same threat actor, who goes by the name Tea Pot (aka teapotuberhacker).

Uber, for its part, has pinned the breach on an attacker (or attackers) that it believes is associated with the LAPSUS$ extortion gang, two of whom are facing fraud charges.

- Optus notifies customers of major incident

Source, Optus

Following a cyberattack, Optus is investigating the possible unauthorised access of current and former customers' information.

Upon discovering this, Optus immediately shut down the attack. Optus is working with the Australian Cyber Security Centre to mitigate any risks to customers. Optus has also notified the Australian Federal Police, the Office of the Australian Information Commissioner and key regulators.

“We are devastated to discover that we have been subject to a cyberattack that has resulted in the disclosure of our customers’ personal information to someone who shouldn’t see it,” said Kelly Bayer Rosmarin, Optus CEO.

The ASCS (Australian entity) provided additional guidance on how to stay safe — link here.

Learn more about my Cloud and Security Projects: https://linktr.ee/acamillo

Consider subscribing to Medium (here) to access more content that will empower you!