Why leave PRT

I think

Recent cyber news

Midnight blizzard RDP spear phishing (Russian)

- Emails contained a Remote Desktop Protocol (RDP) configuration file signed with a LetsEncrypt certificate.
- RDP configuration (.RDP) files is configured to establish a successful connection to an RDP server when executed
- The RDP file is preconfigured to enable local filesystem via tsclient
- With the filesystem, the attackers drop the RATs into AutoStart folders

Mamba 2FA:

- Phishing as a service
- Utilizes Adversary in the middle AITM, usually carried out via Evilginx rather than Gophish
- Evilginx creates a man-in-the-middle where it proxies requests to and fro the actual website.
- Evilginx is used to steal session cookies to gain access to web outlook
- It trivially bypasses 2FA defenses except for FIDO2 authentication
- It is difficult to find defend against this attack (referrer header does not work). A few things that can be checked is if the geo-ip of cookie changes.

Golden Jackal Airgap breach via USB

Salt Typhoon (China)

Recent exploits

Windows IPv6 RCE

Linux CUPS RCE

Remote Registry Service Elevation of Privilege

Ivanti VPN deserialization

PetitPotam (EFSRPC)

- <TBC> Event IDS

PrintNightmare (Spooler service)

- A

PrintSpoofer

OSI

Physical: Ethernet, Bluetooth, Wifi

Data link: MAC Address

Network: IP Address

Transport: TCP/UDP

Session: NetBios/PPTP

Presentation: SSL/TLS

Application: HTTP, FTP, SMB

Triaging alert

Triaging is used to determine the priority and urgency of an alert so that

- Categorize based on factors such as affect asset: UAT vs PROD server affected or attack stage: is it in reconnaissance phase or initial foothold or privilege escalation or lateral movement
- Prioritize: Phishing attempt vs Directory Traversal attempt. The impact of a successful phishing attempt would be more severe than a directory traversal attempt, which would be file disclosure at best. As such, the phishing alert will be prioritized.
- Analyze the alert to rule out false positives:
- Incident response

Business Email Compromise playbook:

In an BEC, how would you identify the IOCs and contain this. How would you ensure this will not happen again.

To analyze,

- I'll first perform legitimacy checks on email subject and body for lookalike domain attempts.
- Next, check for email spoofing by inspecting the email headers for SPF and DKIM records.
- Next, identify any malicious links and attachments.
- For links, use domain reputation like Cisco Talos to check if the domain is new or categorized.
- For attachments, inspect with a sandbox; for PDFs check for embedded links, for MS Office files check for embedded macros. For executables, can perform further analysis with Ghidra to decompile into pseudo code to understand what's it doing.

To contain,

- Check other users who may have received it and quarantine the email if possible.

For recovery,

- Remove attachments, reset compromised passwords, enable SPF DKIM
- Restore device with Golden Image.
- Update the email filter to prevent similar occurrences in future.Windows Event logs

- 4624: User successfully logged on to a computer

- 4688: Process creation

-

- 4625: User failed to logged on to a computer

- 4720: A user created

Malware playbook

What are the IOCs you look for the check if your EDR has been bypassed, and what would you afterwards.

To analyze:

- I'll first check for indicators of compromise (IOCs) such as
    - Files, Processes, Services, Registry, Start Folder, WMIC, Users
- Sandbox analysis
    - Check for network connection attempts
    - Decompile with tools like Ghidra to examine behavior. Strings the executable to extract more IOCs such as URLs
    - Check usual suspicious windows api calls to allocate a huge stub of RWX memory space i.e., VirtualAlloc, VirtualProtect, WriteProcessMemory

To contain:

- Check for scale of impact by pumping in the IOCs into EDR or Splunk to check for presence of the malware through hash or hits to identified malicious domains
- Isolate the workstations

To recover:

- Reset user passwords, restore workstation with golden image, if not possible remove all malware artifacts and perform EDR scan before reconnecting to network.

Data breach playbook:

-

Other questions

How would differentiate a relay attack vs PTH.

In a relay attack, the protocol used is Net-NTLMv2 whereas in a PTH attack it's using NTLM

If a threat intel report warns of a malware along with impact, what would you be end to end process.

What are some MX protections?

What are some suspicious ports that will catch attention?

Random port 4444, telnet port 21 suddenly open on a server its going to be odd.

SOAR Security Orchestration, Automation, response

Splunk SOAR, aka Phantom is used as an automation tool. For example, if a high-fidelity alert fires for unauthorized geo remote access, we can configure it to automatically block the access.

What to do if there is a zero day in a product

- First check if we are affected, look at our CMDB like verum to see if any of our tech stack uses this product.
- If we are affected, for example in the Ivanti VPN deserialization vulnerability. Check if there is a patch or workaround available.
- If no workaround, deploy a WAF block to temporarily disable connectivity to affected service.
- In the case of Ivanti, need to look for alternative solutions