OOTW 04/24/2023

Monday, April 24, 2023 9:17 AM

"Hey everyone, welcome to a another addition to the Out of the Woods Threat Hunting podcast. This is Scott Poley, here with Lee Archinal and This weekly segment features the top 5 stories that threat hunters need to be thinking about, as well as our thoughts on the subject and hunting strategies.

With that, let's dive into the Top 5 Threat Hunting Headlines for the week of Apr 24th 2023!"

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/xtrader-3cx-supply-chain

X_Trader Supply Chain Attack Affects Critical Infrastructure Organizations in U.S. and Europe

The initial supply chain vector that of X_Trader that led to the 3CX supply chain attack which seems that Symantec's hunt teams were able to identify 2 critical infrastructure orgs in Energy and 2 in financial trading.

For heavily guarded more mature infrastructure, this seems like the most effective vector --- not a fan of compliance specific things per say --- and not sure if there is a requirement if you distribute software --- but some of the onus should be put on the software provider and maybe a defined process that "supply chained" tagged individuals need to follow

Example --- we needed for compliance reasons have a process to validate software downloaded and run in secure environments --- well depending on the vendor, validation was different which makes making a good consistent process that is highly effective and followed difficult --- so maybe efforts shouldn't be on how companies validate, but of those companies that distribute and standardized processes of validation

One of the biggest tell tale signs is DLL sideloading --- so with that --- being

able to see DLLs drop alongside EXEs that don't originate from standard install packages in normal directories can be telling. One of the main challenges here is telemetry and aggregation --- not all tools equal with telemetry --- but you can configure Sysmon to capture those types of events.

https://www.fortinet.com/blog/threat-research/evil-extractor-all-in-one-stealer

EvilExtractor – All-in-One Stealer

EvilExtractor is an attack tool targeting windows operating system that relies heavily on PowerShell. It also appears to operate over an FTP service.

Be aware of Outbound FTP communications in general also look for the deleting or stomping of the PSReadline directory which effects cmdline history

https://latesthackingnews.com/2023/04/24/lockbit-ransomware-aims-to-target-macos-systems-but-may-not-be-as-successful/

- https://objective-see.org/blog/blog_0x75.html

Lockbit Ransomware Aims To Target macOS Systems – But May Not Be As Successful

Looks like Lockbit has released version that targets Macs ---- the code it self is very much reused because from analysis it still contained windows, linux, and esxi strings in the bin. macOS will likely join the fray --- and maybe it will adjust some large market targets. I using think of movie, music, and graphic design/marketing firms having big mac presence and lots of money. May not be highly accurate statement, but just where my mind jumps.

Great analysis pivoting to the objective-see blog in the article. Really walks through different mac components and shows the malware is a ways away from being highly effective based on some of the native controls that exist in mac and file access and execution. I did like the list of commandline args that are present for. Lockbit that I wasn't previously aware of. I typically

start at places like that when I want to hunt certain behaviors of execution. Unfortunately no example patterns were provided but good knowledge to have when targeting a malware.

https://cybersecuritynews.com/threat-hunting-tools/

20 Best Threat Hunting Tools – 2023

An interesting list of Threat Hunting tools --- some I haven't heard of mainly because I pay more attention to free tools first. Always good to get pros and cons list by tool to help inform decisions or make you think about your current tool sets.

https://github.com/infosecB/LOOBins

Living Off the Orchard: macOS Binaries (LOOBins)

Everyone has seen the Living Off the Land for Windows and Linux, and now there is macOS. Understanding LOLBins has become imperative in a threat hunter's knowledge base because adversaries rarely don't use any LOLBins in while present in an environment. Understanding macOS's will help defend against targeted attacks, but also looking at them early depending on visibility will also help profile before hand and build additional knowledge around LOOBins.

Hunting for Impact Apr 26nd 12-1pm EST
Hands on hunting with Lee Archinal using real data and tools

"Thanks Everyone for joining our Out of the Woods Threat Hunting Podcast. Looking forward to syncing back up next week.
With that, that closes out our Top 5 Threat Hunting Headlines for the week of Apr 24th 2023!