OOTW 11-7-2022 - Notes

Monday, November 7, 2022 8:33 AM

https://www.cyberscoop.com/insurance-giant-settles-notpetya-lawsuit/

Insurance giant settles NotPetya lawsuit, signaling cyber insurance shakeup

Cyber Insurance still not covering the overall impact costs

- Loses $1.4 billion compared to the $100 million payment

Act of War versus Collateral Damage

- Seems like 'Act of War' is not typically covered
- If it can be proven to be 'Collateral Damage', then it looks like insurance is forced to pay out

This can be a fuzzy area for Critical Infrastructure because they could be the intended target for effects, even though they aren't the target for operational success. This will make negotiating Cyber Insurance tougher in the future because Cyber 'attacks' frequency at least stay consistent if not always slightly increasing -- so insurance companies will have to figure out what they will cover. Obviously deductibles are a thing

So what happens if an attacker is able to come back and attack a company more than once, does that constitute as negligence from the insurance companies eyes --- I mean persistent means persistent --- so that is a likely scenario.

https://thehackernews.com/2022/11/robin-banks-phishing-service-for.html

Robin Banks Phishing Service for Cybercriminals Returns with Russian Server

Phishing as a Service - Robin Banks

- We've mentioned similar services before
- An interesting statement in the article was around how "Cloudflare disassociated Robin Banks phishing infrastucture from its services, causing a multi-day disruptions to operations"

    - Might speak to how active the service is
- Picked up by Russian Provider --- DDoS-Guard (seems to host other sites in Russian interest)

Makes me think of Geo-Blocking --- so when I see malicious services switching to a place that is less likely to respond to take down requests --- I might want to consider blocking their subnet(s) --- in this case they have a few scattered around the world --- so if you concerned with Russian influence and operations --- you may want to look not at just geo blocking 'Russia' but think of services/IT businesses/Hosting that is tied to Russia --- or any other country of concern as well --- do be blind to just geolocations and IP addresses/subnets

- Also uses AdSpect
    - It works as follows: visitors (traffic of any kind: ads, e-mail, organic, etc.) get their intrinsic attributes collected and evaluated by our special PHP script before getting to their final destination. Adspect runs more than a hundred checks on each click and produces a verdict whether a visitor is relevant or unwanted. Relevant visitors are brought to your actual money-making content (the so-called “money page”) whereas unwanted visitors are shown a different version of content that does not expose anything sensitive (the so-called “safe page.”) What to consider “sensitive” is your private choice: *traffic does not cross Adspect servers directly,* so we enforce no policies regarding its nature.

Enables specific targeting and anti-analysis

https://thehackernews.com/2022/11/researchers-uncover-29-malicious-pypi.html

Researchers Uncover 29 Malicious PyPI Packages Targeted Developers with W4SP Stealer

W4sP stealer injected in python packages

- list of offending packages is as follows: typesutil, typestring, sutiltype, duonet, fatnoob, strinfer, pydprotect, incrivelsim, twyne, pyptext, installpy, faq, colorwin, requests-httpx, colorsama, shaasigma, stringe, felpesviadinho, cypress, pystyte, pyslyte, pystyle, pyurllib, algorithmic, oiu, iao, curlapi, type-color, and pyhints
- Used typosquatted domains of the real package locations

- Used typosquated domains of the real package locations

A Look at the pacakge (https://github.com/loTus04/W4SP-Stealer/blob/main/wasp-1.1.6.py)

- Makes calls to https://api.ipify.org to learn victims IP address
- Makes calls to https://geolocation-db.com/jsonp/<ip> to learn geolocation data
- Discord Calls
  - https://discord.com/api/v6/users/@me/relationships
  - https://discord.com/api/users/@me/billing/payment-sources
- Hardcoded : User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
- Uploads stolen data via discord cdn
- Uploads stolen files to gofile.io
  - https://{requests.get("https://api.gofile.io/getServer").json()["data"]["server"]}.gofile.io/uploadFile
- Intalls Run key for persistence
  - "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
  - Name: SecurityHealthSystray.exe

Always important to validate sources of code --- and be able to skim code for interesting artifacts --- I look for web call infor --- certain directory path refs ---- registry refs --- interesting file extensions --- possible calls for execution/cmdline --- and if any code looks to be really obfuscated

When making discoveries on how to detect malware --- take into account the difficulty of changing a capability in the malware is to determine what would be more a behavior or IOC (i.e. webcalls vs UserAgent)

https://therecord.media/microsoft-accuses-china-of-abusing-vulnerability-disclosure-requirements/?web_view=true

Microsoft accuses China of abusing vulnerability disclosure requirements

This is concerning

- China forcing companies/individuals to disclose vulnerabilities to the government prior to public/vendors --- obvious there was a concern initially that China would leverage this preknowledge in their cyber operations, which is why Homeland Security Department's Cyber Safety Review Board "spoke with the Chinese Government" to determine foul play and didn't find anything

- This needs to be validated with data --- conversations don't provide anything other than what the participants want you to hear

Microsoft gets hit about not being strongly tied with security --- but I feel differently --- they now have the most visibility from a data point perspective with having defender existing as a good core Endpoint Protection --- and have made great strides in understanding the data/telemetry that aids in their intel and security operations

(https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us)
Their data speaks differently to how China is behaving with advanced knowledge

- On average
  - takes 14 days for an exploit to be available in the wild
  - Takes 60 days for POC code to release on github
  - Takes 120 days to be available in scanning tools
- Examples of exploits built and utilized by China's APT before being known believed to be correlated to new policy imposed sept 2021
  - SolarWinds Serv-U
  - Zoho ManagerEngine ADSelfService Plus
  - Zoho ManageEngine ServiceDesk Plus
  - Microsoft Exchange
  - Confluence

https://www.malwaretech.com/2022/11/everything-you-need-to-know-about-the-openssl-3-0-7-patch.html

Everything you need to know about the OpenSSL 3.0.7 Patch (CVE-2022-3602 & CVE-2022-3786)

Good Write-up of the effective risk

- PunyCode used in the emailaddress field in the X.509 cert allows for buffer overflow --- crashes crypto service/binary
- More a client side since it has to do with the certificate verification which typically done by clients, but the cert must be signed by a trusted CA to get this point
- Server side risk --- CA requirements usually aren't required by servers --- and for a server to be at risk it needs to be configured to allow client

authentication in this manner

Something to note about DoS vulnerabilities --- when it comes to software they commonly are tied to corrupting/rewriting areas in memory or on the manipulating or overflowing the stack --- depending on how far you can move on the stack or rewrite parts of the stack, how much you can write in memory and where --- can lead to remote code execution

It's a good idea to know when your encryption software crashes or fails --- and now if people are looking more into other weakness like this --- you might see more of this --- so checking out what we have on Hunter

OpenSSL Application Spawned Windows Error Reporting - Potential OpenSSL Exploit and Crash Attempt

OpenSSL Application Crashed Associated With Crypto Related DLL - Windows Event Log

EventId: 1000