COMPUTER SECURITY UPDATE

LIVIU VÂLSAN
FOR THE CERN COMPUTER SECURITY TEAM

HEPIX SPRING 2021 ONLINE WORKSHOP

This is not a resurrection of past Computer Security talks

LARGE SCALE ATTACKS

- Supply chain attacks.
- Chain of zero day vulnerabilities affected popular software components usually exposed on the Internet.
- Attacks targeting tens of thousands of organisations
- Academia not spared, on the contrary.
- “Interesting” organisations being delivered additional malware.

SUPPLY CHAIN ATTACKS – SOLARWINDS (1)

- Initially discovered by FireEye in Dec 2020 during Incident Response of their company breach.
- SolarWinds was compromised in early 2020.
- Attackers added a backdoor to a key library that is part of SolarWinds.
- SolarWinds' Orion product released between March and June of 2020 were affected.
- A compromise of this platform may affect all parts of a network that are controlled by Orion.

SUPPLY CHAIN ATTACKS – SOLARWINDS (2)

- SolarWinds has over 300,000 customers including much of the US Federal government including the Department of Defense, 425 of the US Fortune 500, and lots of customers worldwide.
- ~33,000 customers were using Orion out of which ~18,000 had a backdoored Orion version.
- Targets likely ranked by perceived strategic value and the relative likelihood that exploiting them might result in the entire operation being found out and dismantled.
- Additional persistence mechanisms to access to victim networks were put in place for interesting targets beyond the initial backdoor.
- Microsoft source code accessed as a result of the SolarWinds breach.

SUPPLY CHAIN ATTACKS - CENTREON

- SolarWinds is not the only network monitoring sw targeted.
- French software provider Centreon also breached.
- CentOS based, open source version available as well.
- First victim compromised late 2017 with the campaign lasting until 2020.
- The campaign mostly affected information technology providers, especially web hosting providers.
- The campaign bears similarities with previous campaigns attributed to the intrusion set named Sandworm

MICROSOFT EXCHANGE 0-DAY EXPLOITS (1)

- Multiple 0-day exploits being used to attack on-premises versions of Microsoft Exchange Server.
- Exploitation provides access to email accounts and allowed installation of additional malware to facilitate long-term access to victim environments.
- At least 10 APT groups have exploited the flaws.
- The surge in hacking suggests multiple sets of espionage groups had access to the software exploit before Microsoft released fixes for it on March 2nd 2021.

Microsoft Exchange 0-day exploits (2)

- Proof-of-concept tool to hack Microsoft Exchange servers that combined two of those vulnerabilities published on GitHub
- Strong indications that all affected servers were compromised.
- If you are running an affected Exchange server exposed to the Internet it's almost certainly compromised by multiple actors.
    - Ransomware attacks expected.
- The victim list contains 86,000 IP addresses of Exchange servers worldwide, with 30,000 organisations in the US alone.
- Check My OWA: https://checkmyowa.unit221b.com/
- Official nmap script from Microsoft to check if you are affected

SECURING MICROSOFT EXCHANGE

- Avoid having the service publicly exposed, for example by putting it behind Single Sign On or VPN.
- Configuration hardening, e.g. restricting the binaries that can be executed; restricting the outgoing network connections.
- Have anti-malware / EDR protection in place with behavioural analysis.
- Keep the entire software stack updated.

HPC ATTACKS

- Different global attacks involving both complex and sophisticated malicious actors.
- ESET named one of the malware components "Kobalos” and released their analysis.
- Article focuses on only one of the malicious tools in the toolset, used in one wave out of four, all leveraging different tools, techniques and procedures.
- Very strong signal that sophisticated malicious actors will invest significant effort in writing custom malicious software to target our sector.

TCP/IP STACK VULNERABILITIES

- At least nine embedded TCP/IP stacks (and their variations) that were found vulnerable during the AMNESIA:33 and NUMBER:JACK research.
- Impacting tens of millions of IoT, OT and IT devices.
- These vulnerabilities primarily cause memory corruption, leading to remote code execution, denial-of-service attacks and disclosure of sensitive information.
- Recommended mitigations
  - Identify devices running the vulnerable stacks.
  - Patch when possible.
  - Segment to mitigate risk.

CPU SIDE CHANNEL ATTACKS

- Exploits for old side channel attacks start being seen in the wild, e.g. for Spectre
- Included in exploit packs such as Immunity Inc's CANVAS, which was publicly leaked
- New side channel attacks continue to be announced, e.g. Lord of the Ring(s): Side Channel Attacks on the CPU On-Chip Ring Interconnect Are Practical

SUPPLY CHAIN ATTACKS FOR OPEN SOURCE SW

- Software today has become an assembly of components from a wide range of sources: developed in-house, acquired from third-parties, or downloaded from free and public sources.
- Open-source projects have an average of 180 package dependencies.
- Dependency confusion: in case a package exists both on the internal package repository and externally (such as on pypi, npm, etc), the default is to install it from the source with the higher version number.
- Proof of Concept used against Apple, Microsoft and dozens of other companies.

SUPPLY CHAIN ATTACKS FOR OPEN SOURCE SW

- Possible mitigations include:
  - Only allow installation from an internal repository manager, such as Nexus or Artifactory.
  - Do not rely on the programming language's package manager but package the modules into distribution specific packages (RPM) after (automatic) code audit.
  - Perform auditing of packages coming from public sources as well as in house developed code using tools such as Snyk.

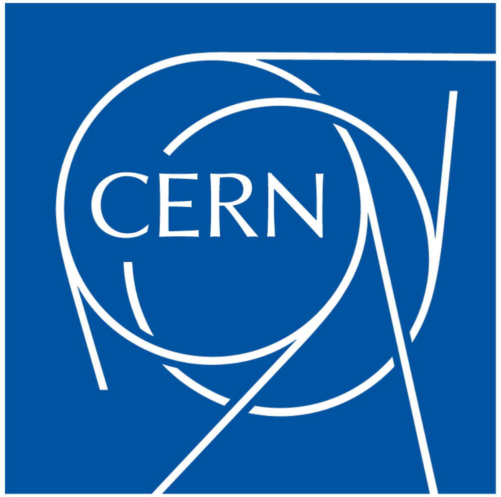
CONCLUSIONS AND RECOMMENDATIONS

If we want to ~~**win**~~**/keep up with this marathon**, we should/must(!)

- More often **choose "security"** instead of "convenience";
- More often **consider "privacy"** instead of "freedom";
- Have good configuration management for **prompt and agile patching** (office computing, data centre *and* control systems);
- Have deep direct **ties with the community** to learn quickly about the malicious evil (and where they affect / attack us);
- Have good **traceability & logging** in place to figure out where we are attacked / affected;
- Accept that we do not and cannot control the full phase-space. Protection is often difficult/impossible, and - for sure - costly.

WLCG SECURITY OPERATIONS CENTERS WG

- Working group designed to enhance site security monitoring
  - Network monitoring
- Coupled with threat intelligence and real time search capabilities
  - Minimally viable Security Operations Centre
- Resources:
  - Website
  - Documentation
  - Mailing list
  - Access to Academic MISP instance


CERN