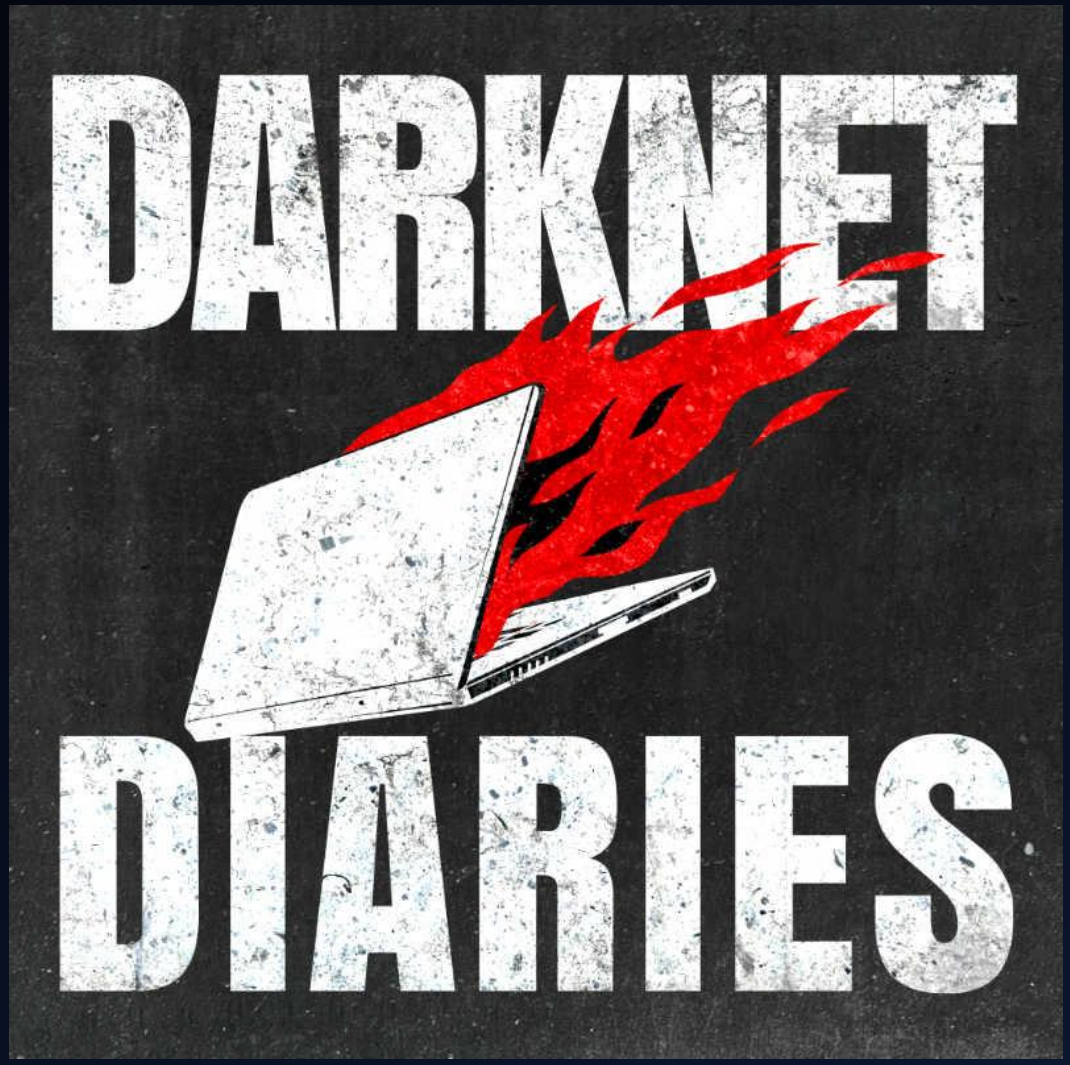
CASE STUDY

Courtesy of :
Darknet Diaries
Ep: 103 Cloud hopper



By: M. Muzni

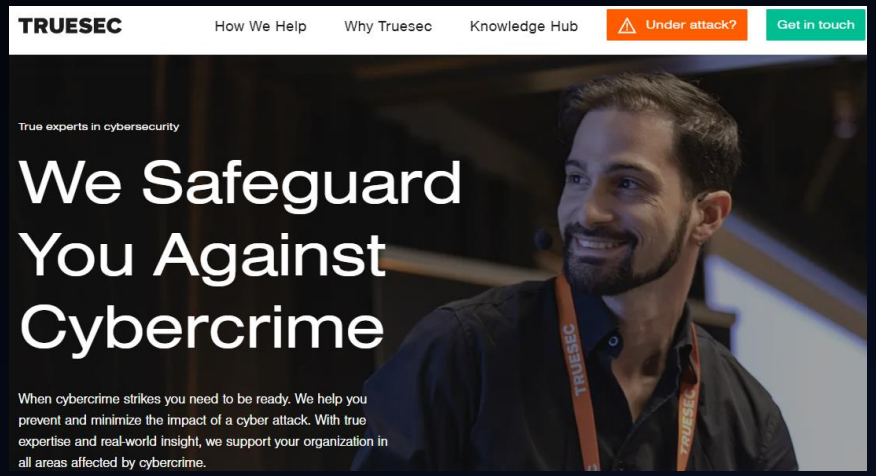
Who is the most powerful person in a Company?

CEO

SYSTEM ADMINISTRATOR

JANITOR

2016 – Swedish Sec. Service Tips off TRUESEC



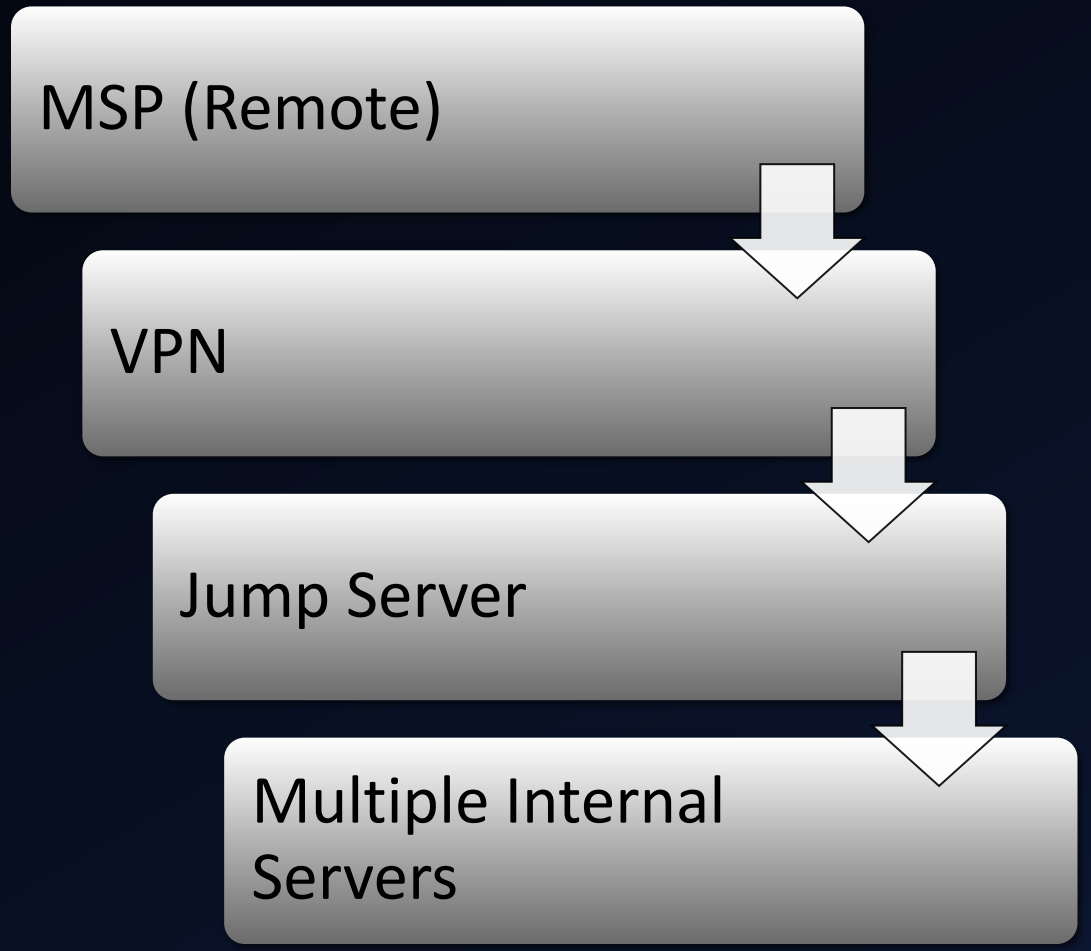
- **Swedish Client** - Typical large enterprise org. with thousands of computers | Remotely Managed by an **MSP** (Managed Service Provider).

- **Jump Server** Talks to a command and control in another country.

- Two IPs of Command in Control Servers that client's infrastructure was communicating with
- Time Windows of when the connections started and ended
- Clients Internal Host name and IP address that was suspected to be the infected server

MSP Managed Client

MSP is a Multination company had thousands of client in 12 countries



FORENSICS INVESTIGATION

Disk image – exact copy of the hard disk

Memory dump – copy of the RAM which copies any running Malware as well.

- Mounted the external Hard Disk as Read-Only.
- Auto Scan takes hours to detect so carried out manual check
- **C:\Temp** – best place to check first
- Found an output file **Hostnameoftheserver.mimicatz.hash** with 100's of credentials users logged in to this server ever in clear text. (Not Hashed)
- Including several Active Directory Administrators
- The issue was immediately escalated | Business Leaders called in

Findings

Something you can get out from memory is network connections. Current or historical, if there is still left in memory somewhere.

VBA 32 8rkit.exe = Legitimate software Called VBA 32 anti rootkit scanner

VBA328rkit.exe was in a very unusual location

it was under **C:\Windows\web**. Which is a folder that exists. But it doesn't have that type of software in there. So just having that binary located in that directory was strange. And next to that file, there were another few file, a couple of DLLS, another couple of files.

DLL Sideloading Attack – Very well-known technique and very effective

Findings Cont..

3 types of DLL sideloading Malware

Connecting to different Command in Control servers in different points in time

Time stamps of this DLLL sideloading execution goes months back

search widened in to 2 directions

Memory Analysis

Do Not to shut down & wipe off the compromised server immediately

Further memory analysis found someone remotely logged with valid credential and dumped a malware

Found a note in the Malware analysis & found a note for the Forensics Investigators

EP. 2 -1:29 – 2.20

Have your bosses given you the space try to be a hacker..? Common man don't kill me.

Found more interesting evidence

Executable **nbt.exe** = which is a legitimate tool to scan **NetBIOS** scanner

p.Txt – was an empty txt file

Batch file called **pp.cmd** >> had 33 line each line was commands executing **nbt.exe** (NETBIOS scanner) followed by a public IP range address and then put the output in to the p.txt file

Had **33 public IP address ranges** on that batch file that was scanned|

Found these public IP address ranges **19 of those are belong to US Department of Defense**

Few weeks later the **Nation State Actor** logged back in to the Jump Server with whole lots new tools including a known malware and DLL files which talked to a totally new command in control server.

known malware which **PLUGX** is a known **RAT** (Remote Access Trojan)

MSP Breached

Three Weeks later MSP confirms they had been hacked into and didn't know it until TRUESEC (Fabio & his team) showed them the evidence for them.

This must have been a really bad day for the MSP to discover.

In weeks, More of their customers have been compromised with the same Malware.

MSP had privilege access to some US Gov. Agencies networks

Reuters journalists Jack Stubbs, Joseph Manning Christopher Bean did an investigation and found that seven different service providers were compromised and they listed Hewlett-Packard Enterprise, IBM, Fujitsu, Tata Consultancy, entity data, dimension data and Computer Sciences Corporation.

Press Release

Deputy attorney general Rod Rosenstein and FBI director Christopher Wray are announced indictments on two Chinese hackers for their alleged roles in a global hacking campaign.

APT 10 compromised MSP clients Data from 12 countries.

https://www.fbi.gov/wanted/cyber/apt-10-group

ONE OF THE MOST SOPHISTICATED DATA BREACHES OF ALL TIME

APT 10 compromised the data of MSP clients located in 12 countries
Brazil, Canada, France, Finland, Germany, India, Japan, Sweden, Switzerland the United Arab Emirates, the United Kingdom and the United States

the defendants hacking campaigns also targeted US government agencies including the laboratories of NASA the United States Department of Energy and the US Navy members

APT 10 stole personal confidential information including Social Security numbers and dates of birth from over 100,000 Navy personnel

American companies and government agencies spent years of research and countless dollars to develop their intellectual property while the defendants simply stole it and got it for free

News

REUTERS World Business Markets Breakingviews Video More

CYBER RISK JUNE 26, 2019 / 11:04 PM / UPDATED 3 YEARS AGO

Exclusive: China hacked eight major computer services firms in years-long attack

By Jack Stubbs, Joseph Menn, Christopher Bing 4 MIN READ

Technology Review Featured Topics Newsletters Events Podcasts

Computing Dec 20

Chinese hackers allegedly stole data of more than 100,000 US Navy personnel

That's one of the stunning allegations against two Chinese government hackers in an indictment issued today by America's Department of Justice (DOJ).

The news: The indictment accuses the two hackers, Zhu Hua and Zhang Shilong, of working for a group with links to China's Ministry of State Security, the country's main intelligence agency. Dubbed Advanced Persistent Threat 10, or APT 10, by security researchers, the group mainly aimed to steal intellectual property, but it also scooped up information about US military personnel, including Social Security numbers, dates of birth, and salaries. The US Navy reportedly has somewhere around 330,000 active duty members, so the hack likely affected a significant percentage of them.

REUTERS INVESTIGATES | Dark Clouds

A REUTERS EXCLUSIVE

Inside the West's failed fight against China's 'Cloud Hopper' hackers

CLOUD HOPPER: Major corporations, from IBM to Hewlett Packard Enterprise to Fujitsu, were invaded by Chinese cyber spies, Reuters found. Illustration by Catherine Tai/REUTERS

Eight of the world's biggest technology service providers were hacked by Chinese cyber spies in an elaborate and years-long invasion, Reuters found. The invasion exploited weaknesses in those companies, their customers, and the Western system of technological defense.

THE WALL STREET JOURNAL.

TECH

Ghosts in the Clouds: Inside China's Major Corporate Hack

A Journal investigation finds the Cloud Hopper attack was much bigger than previously known

By Rob Barry and Dustin Volz
Dec. 30, 2019 1:04 pm ET

REMEDIATION

Thousands of Active Directory (AD) user account credentials (password) had to be reset.

Some of these AD account are privileged users accounts tied to other networks .

In-house developed applications had to be decommissioned & replaced.

EDRs needs to be deployed across all systems and continuous monitoring.

Company cut ties with the current MSP & replaced with another.

KEY POINTS

MSP's are pretty common. More and more companies are outsourcing their IT infrastructure, so to target them makes a lot of sense.

If your goal is to steal intellectual property, it's sort of like going out to the janitors key ring, which can get you access into many buildings in town

If your goal is to steal intellectual property, it's sort of like going out to the janitors key ring, which can get you access into many buildings in town.

REFERENCE

https://podcasts.google.com/feed/aHR0cHM6Ly9mZWVkcy5tZWdhcGhvbmUuZm0vZGFya25ldGRpYXJpZXM/episode/NTgyMWVhYzItYmMxMS0xMWViLWJhZGMtYmZmYWI1ZjgyYjVj?ep=14

https://www.csoonline.com/article/3353416/what-is-mimikatz-and-how-to-defend-against-this-password-stealing-tool.html

https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper

https://www.reuters.com/article/us-china-cyber-cloudhopper-companies-exc-idUSKCN1TR1D4

https://www.fbi.gov/wanted/cyber/apt-10-group

https://www.youtube.com/watch?v=277A09ON7mY

https://www.wsj.com/articles/ghosts-in-the-clouds-inside-chinas-major-corporate-hack-11577729061

https://www.technologyreview.com/2018/12/20/239760/chinese-hackers-allegedly-stole-data-of-more-than-100000-us-navy-personnel/

THANK YOU FOR WATCHING.