

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

2017: Cuando el ciberespacio refleja el mundo real



- Antonio Cañada
- FireEye

Índice

1. **Main trends in the CyberSpace**
2. **When Cyber-Criminal used Cyber Extortion & Destruction – FIN10**
3. **Geopolitical impacts in the Cyber Space : APT32 and APT33**
4. **When Nation States espionage impacts countries GDP: APT10**
5. **Take aways and conclusion**

THREAT LANDSCAPE CONTINUES TO EVOLVE

- *Motivations behind the attacks*



Influence

- FireEye observes a change in motivations for certain specific Nation State sponsored group with the aim to influence geopolitical decision.
- The main objectives seen during the US election and during the European election in France, UK or Germany, are to push left right parties and to reduce the confidence in institutions.



Cyber Espionage

- FireEye observes several nation states sponsored groups from different countries including Iran, North Korea and China who are continuing operation and campaign to gain economical advantages.
- All verticals of business are targeted and the campaign are directly linked to the local government strategy of growth.



Financial

- FireEye observes nation states and non nation states groups using APT technics and procedures to win money.
- FireEye observes an approach of stealing high volume in a one off operation versus multiple small quantity.
- FireEye observes also an appetite to target crypto-money and stock exchanges instead of standard financial institutions.

THREAT LANDSCAPE CONTINUES TO EVOLVE

- *Main Vectors used by attackers*



Ransomware

- FireEye observes ransomware infections continuing to grow, with iSIGHT seeing the introduction of over 60 new ransomware families in each quarter of 2017
- The barriers to entry are lowering with enhanced distribution frameworks and Ransomware-as-a-Service
- The attacks continue to be distributed broadly across sectors



Spear Phishing

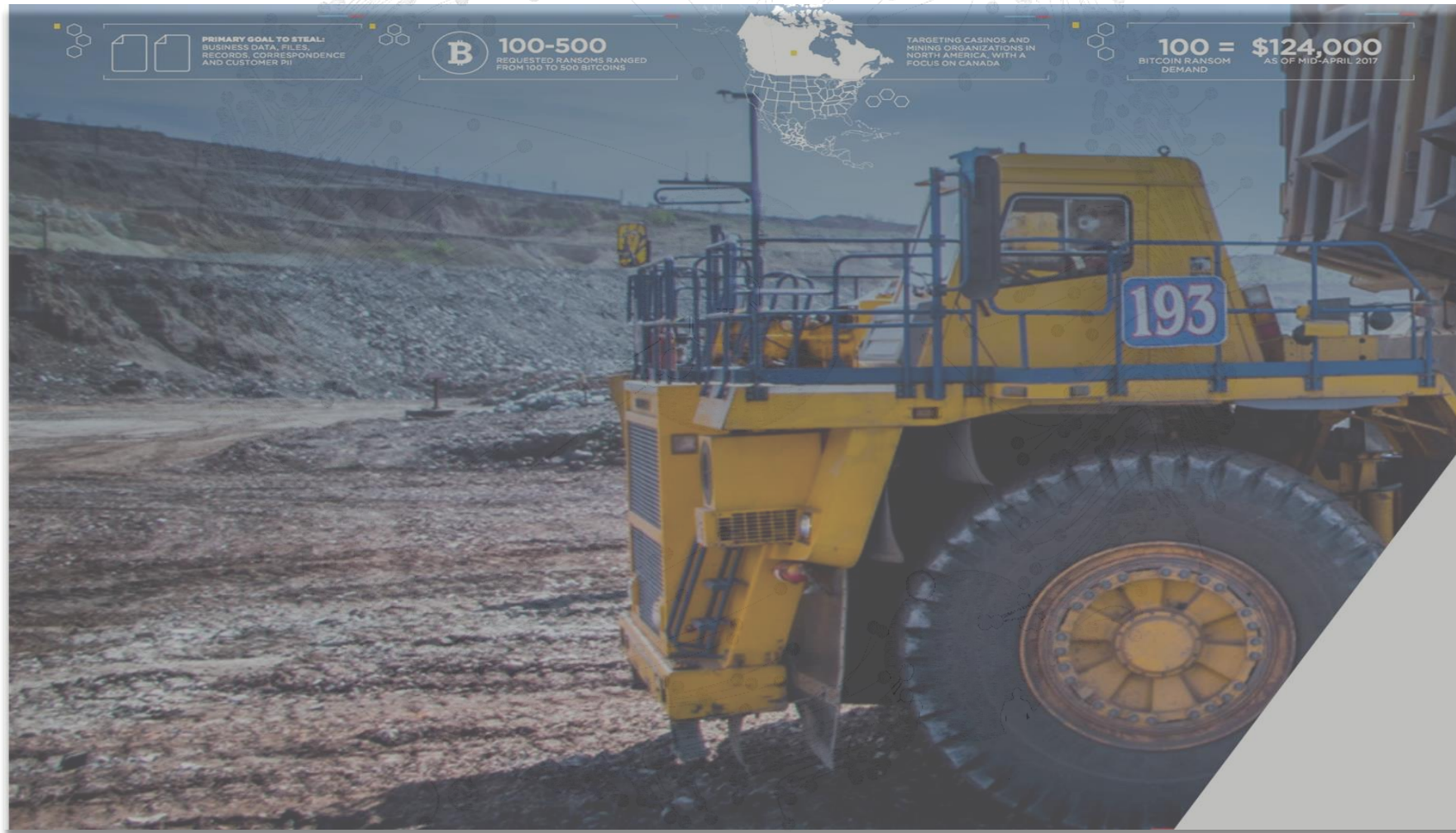
- Spear phishing is still the most common utilized foothold technics.
- Attackers are using targets interest to push them to open a link or an attachment.
- APT33 used Job profiles and Resume on the petrochemical industry as an example.



Authorized tools and supply chain

- FireEye observes a trend in targeted attacks using supply chain as a propagation vector inside the enterprise.
- APT32 used in some cases a McAfee ePO architecture to spread over the network.
- Attackers are becoming adept at Privileged Escalation which allows them to move natively across the environments
- Attackers are using authorized Microsoft tools and command to move laterally and exfiltrate data

When Cyber-Criminal used Cyber Extortion & Destruction – FIN10



FIN 10 OVERVIEW



FIN10 is a financially motivated group that deliberately targets organizations.

Involved in financial crime operations since at least 2013.

Compromises victims' networks to exfiltrate sensitive data.

Uses extortion tactics to monetize operations.



*Main targets are casinos and mining companies located in Canada
Targeted PII, Corporate business Data*

Key findings:

- SpearPhishing with malicious attachment
- Social engineering and specialized lures to attract victims
- Embedded URLs pointed victims' machines to malicious
- Publicly available software, scripts, and techniques. (Meterpreter, Splinter Rat, PowerShell Empire)
- Stolen credential on VPN
 - Schedule Tasks for persistence

FIN 10 OVERVIEW ATTACK LIFECYCLE - TTPs

At this point your company has two options:

1. Meet our demand and pay the one time price of 500 BTC (Bitcoin)
 - all of the stolen data is permanently deleted, none of it gets posted on the internet, your computer network will remain safe and functional and your organization wont be bothered again.
 - Bitcoin transactions are anonymous no one will know you cooperated

Maintain Presence

Lateral Movement

- **Compromised VPN credentials**
- **RDP** →



Co

Establish
ol

Linkedin and social network researches

- Spear Phishing

- Meterpreter function of metasploit
- Powershell empire
- Splinter RAT

- Meterpreter function of metasploit
- Powershell empire
- Splinter RAT

- Powershell empire
- Splinter RAT
- Network traffic capture using OLAP TCP dump driver

- Extortion via False Flag
- Data exposure
- Destructive batch Scripts

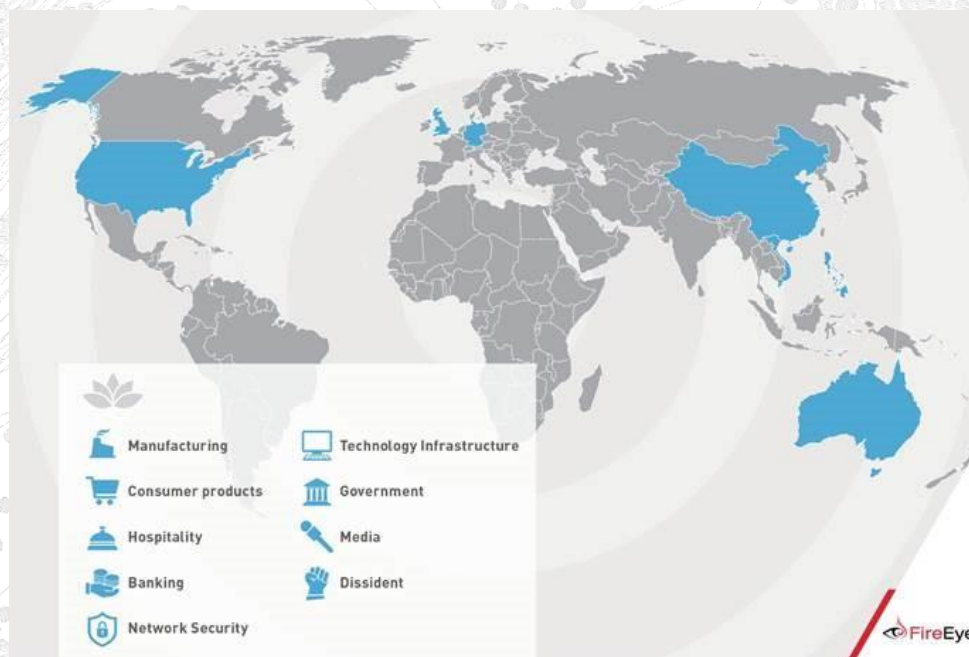
Geopolitical impacts in the Cyber Space : APT32 and APT33



APT32 OVERVIEW



- APT32 is a cyber espionage group aligned with Vietnamese government interests
- 12 victims identified through our worldwide detection sensor network
 - 10+ external victims
- Ultimately 4 groups consolidated into APT32



APT32 targeting of private sector interests in Southeast Asia presents increased risks to consider

APT32 is a threat to activists, journalists, and foreign governments

Key findings:

- Tracking their own activities with dedicated websites
- Usage of advanced multi stages Lures
- High level of obfuscation and high usage of new technics (they monitored twitter/websites or researches)
- Use of third party like ePo deployment task to deploy backdoors and tools
- APT32 uses a custom suite of backdoors spanning multiple protocols

APT33 OVERVIEW



Observed since 2013, with an high activity in 2016, 2017
Artefacts and forensics linked to Iranian persona
Campaign aligned with Iranian interest
One of the 10+ groups we are observing in this region



Main targets are aviation and energy sectors

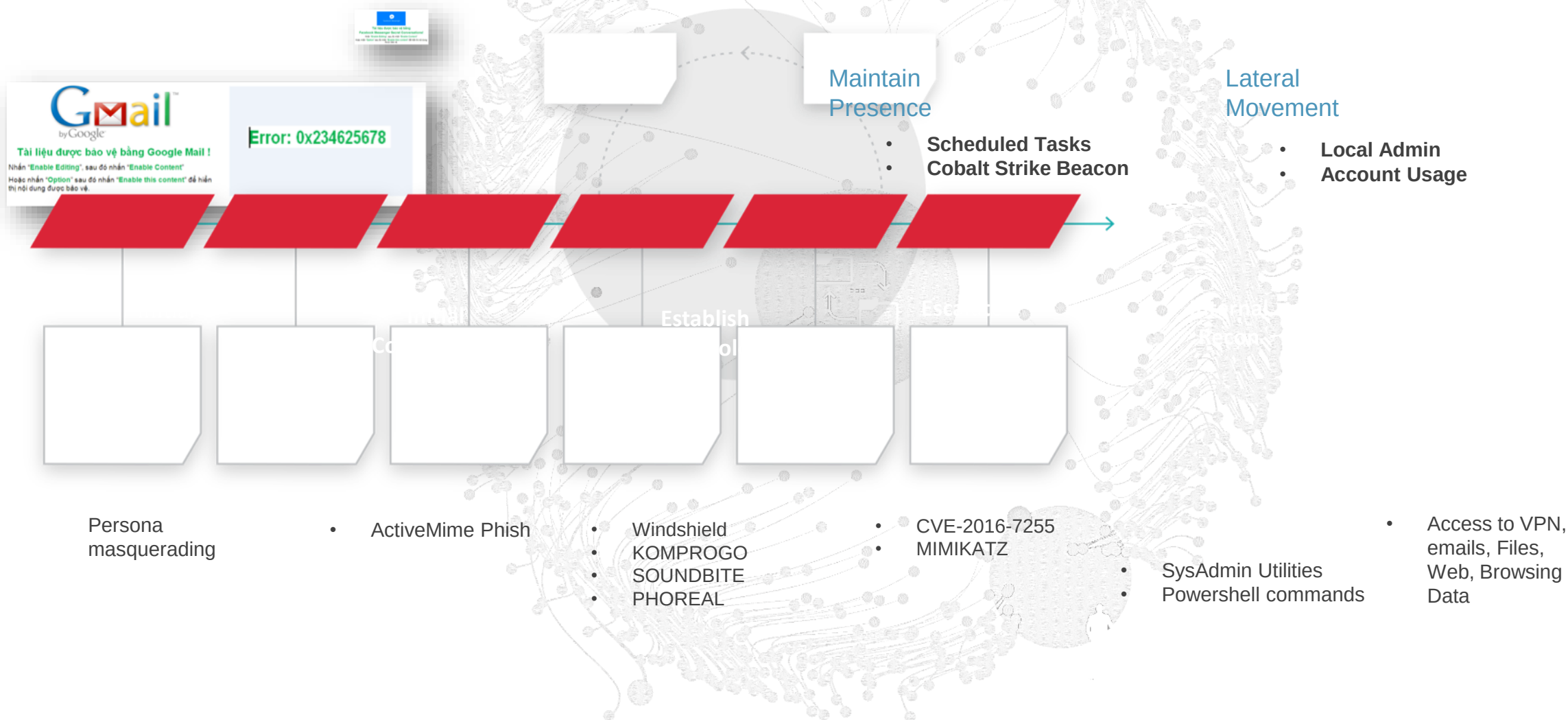


Targeted US, Saudi Arabia, South Korea companies

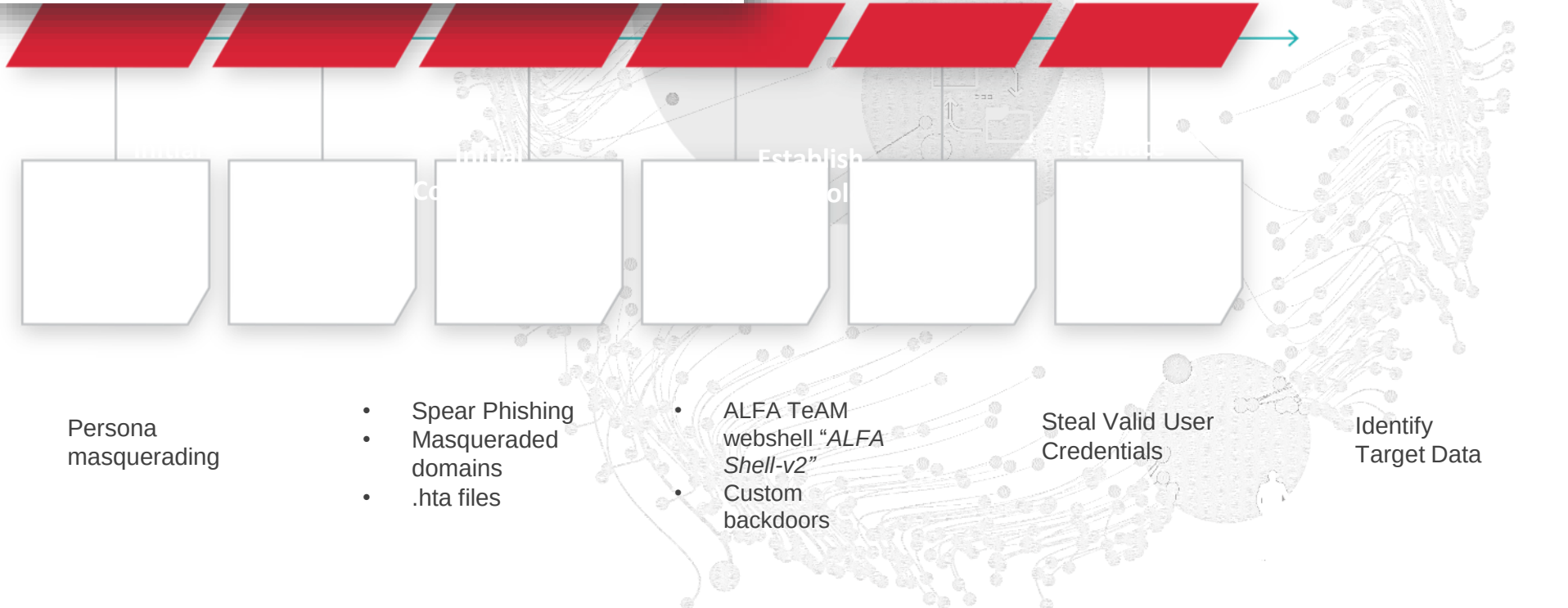
Key findings:

- SpearPhishing and domains masquerading
- Fake job profile and web injection
- Farsi language in the code
- Persona repository discovered during research (Xman_1365-X) on TURNEDUP backdoor
- Use of Iranian-related DNS name servers and hacktivist tool
- Destructive capabilities with SHAPESHIFT

APT32 OVERVIEW ATTACK LIFECYCLE - TTPs



APT33 OVERVIEW ATTACK LIFECYCLE - TTPs

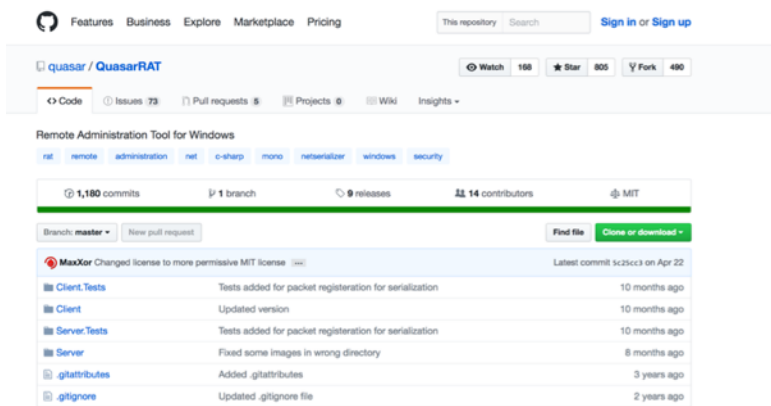


boeing.servehttp[.]com
alsalam.ddns[.]net
ngaaksa.ddns[.]net
ngaaksa.sytes[.]net
vinnellarabia.myftp[.]org

When Nation States espionage impacts countries GDP: APT10



APT10 OVERVIEW



- APT10 (MenuPass Group) is a Chinese cyber espionage group that FireEye has tracked since 2009
- We believe that the targeting of these industries has been in support of Chinese national security goals, including acquiring valuable military and intelligence information as well as the theft of confidential business data to support Chinese corporations.
- In June 2016, FireEye iSIGHT intelligence first reported that APT10 expanded their operations
- **Motivation** – Intellectual Property theft



Targeted Industries – Construction, Engineering, Aerospace, Defense, Information Technology, Healthcare, Telecommunications, Automotive

Targeted Regions – US, UK, Canada, Germany, Japan, Finland, France

At least, 43 confirmed campaigns, ranging from late 2009 to present

Key findings:

- Spearphishing/Lateral movement through MSP as initial compromise
- Use of SOGU/PlugX, BUGJUICE/Redleaves, Quasar RAT as backdoor/foothold
- Use of Mimikatz, WMIExec for credential harvesting and lateral movement
- Use of built-in Windows commands to perform recon and lateral movement
- Use of Windows .CAB files to archive/stage stolen data

Take aways and conclusion



- Cybercriminals are using Nation States capabilities.
- Countries are developing cyber program strategy:
 - Defensive Strategy
 - Offensive Strategy
- High level tools are becoming freely available and used by hackers.
- Visibility and ability to react is key since 100% security does not exist

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en



