SOC ReLoad
#SOCReLoad21

TRACK 2 - OPERATIONS

Developing More Effective Ransomware Playbooks: What We Can Learn From the Latest Attacks to Accelerate Detection and Response

Alex Hinchliffe
Threat Intelligence Analyst

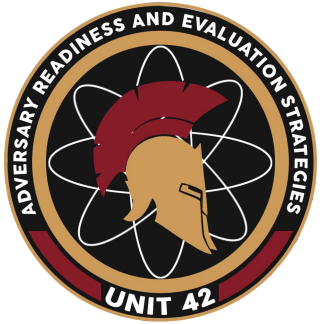
Simon Monahan
Product Marketing Leader

UNIT 42
BY PALO ALTO NETWORKS

PICUS

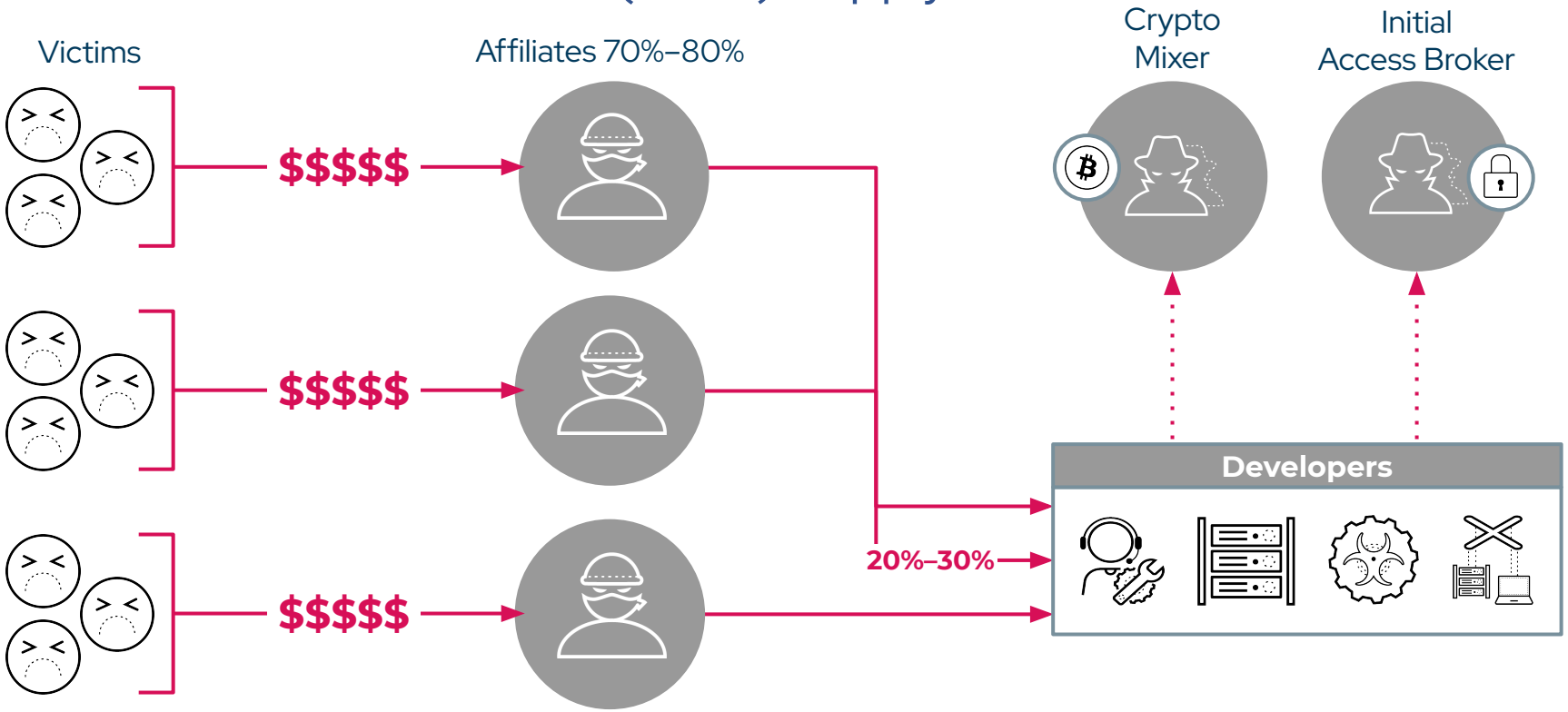
#WHOAMI

- Threat Intelligence Analyst, Adversary Readiness & Evaluation Strategies (ARES), Unit 42
- Background:
  - Mobile Malware Researcher/Lead at Intel Security (Consumer) -> Intel USA
  - Threat Researcher at McAfee Labs (AVERT) -> Intel Security UK
  - Intern at Network Associates Inc UK
- Areas of interest and study:
  - Threat Intelligence & Hunting
  - Geopolitical nature of cyber attacks
  - Malware Research
  - Defence Strategies
  - Toos development



Ransomware Trends

Ransomware-as-a-Service (RaaS) Supply Chain



Ransomware Trends

Software Vulnerabilities

Vendor	CVE	Type
Citrix	CVE 2019-19781	Arbitrary code execution
Pulse	CVE 2019-11510	Arbitrary file reading
Fortinet	CVE 2018-13379	Path traversal
F5 - Big IP	CVE 2020-5902	Remote code execution (RCE)
MobileIron	CVE 2020-15505	RCE
Microsoft	CVE 2017-11882	RCE
Atlassian	CVE 2019-11580	RCE
Drupal	CVE 2018-7600	RCE
Telerik	CVE 2019-18935	RCE
Microsoft	CVE 2019-0604	RCE
Microsoft	CVE 2020-0787	Elevation of privilege
Netlogon	CVE 2020-1472	Elevation of privilege

Top Routinely Exploited CVEs in 2020

Top Routinely Exploited Vulnerabilities

Accellion

VSA™ by Kaseya

Case Study

REvil Ransomware

REvil / GandCrab / Sodinokibi

Ransomware-as-a-Service (RaaS)

Monitored by Unit 42 since 2018

Behind the large-scale Kaseya Attack

REvil Historical Modus Operandi

Mode of Operation	Delivery	Industries	Double Extortion
Targeted	RDP (stolen creds) Phishing	Professional/ Legal, Mfg., Media, Wholesale/Retail, Const./Engr., Energy	Yes

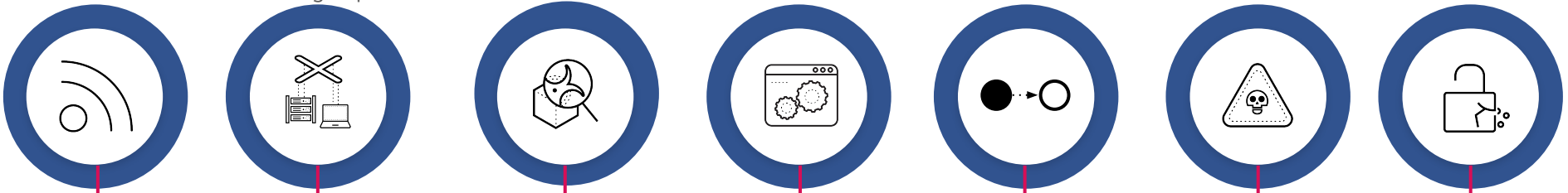
An Evolution In Progress?

+Opportunistic	+Software Vulns	+Any	Maybe

Case Study

REvil Attack Lifecycle from Unit 42

1. Exchange CVE-2021-27065, CVE-2021-26855
2. PuTTY used to add 'admin' to Users, local admin, and Remote Desktop users groups
3. Mimikatz
4. Advanced IP Scanner
   KPort Scanner
   Sharphound
   Net, NETSTAT, IPCONFIG commands
5. RDP
   Cobalt Strike
6. Disabled Windows Defender
7. PsExec to push Ransomware



Case Study
VPN Access

ATTACK OVERVIEW

- The Threat Actor gained VPN access via **admin credentials possibly found on the dark web**
- They established persistence via **scheduled tasks** and **registry keys**
- Post Exploitation frameworks used, such as **Cobalt Strike** and **Powersploit** to further gain a foothold in the environment and establish C2 capabilities to deploy further payloads
- 750GB data exfiltrated using **Rclone** configured to send data to **pcloud** link
- All **Virtual Machines** on the **ESXI server** encrypted and logs wiped
- This attack spanned roughly **2 months** from initial compromise until encryption
- Business continuity restored after several days of downtime and decryption of business critical applications
- Threat Actor was very aggressive in **contacting business clients, employees** about the incident

Extortion Types

Ransomware	Double Extortion	Triple Extortion	Quadruple Extortion
Encrypt victim files, drop ransom note and wait for payment	+ Data exfiltration with threats of release/publication should payment not be made	+ Threat of DDoS attacks to sabotage externally-facing business services (assuming not already affected by encryption)	+ Directly emailing the victim's customers or having contracted call centers contact customers. Possible contact with the media to disclose the compromised organisation

Ransomware Mitigation and Detection Playbooks

Prevention

- Block/disable/monitor external RDP instances
- Block admin tools like PsExec where possible
- Restrict file shares like SMB
- Patch external facing services (e.g. VPNs)
- Depreciate unused external facing servers/services
- Use multi-factor authentication across services
- Build in capabilities to isolate resources
- Facilitate disconnected tape backups
    - Test backups and restoration plans
- Block access to online file sharing applications

Detection & Response

Reconnaissance commands	Net, netstat, ipconfig
Killing processes	net stop, taskkill.exe
Impair defences	regedit.exe, schtasks.exe
Preventing restoration	vsadmin.exe, wmic.exe
Removing evidence	cipher.exe, fsutil.exe, wevtutil
Stopping services	sc.exe
Boot settings	bcdedit.exe
Port knocking	IP Scan, KPort Scanner, etc
Exfiltration and archive tools	ZIP, RAR, Rclone, etc
Tools / applications	PSExec, powershell, etc
Protocols	TOR, pcloud, meganz etc

THANK YOU!