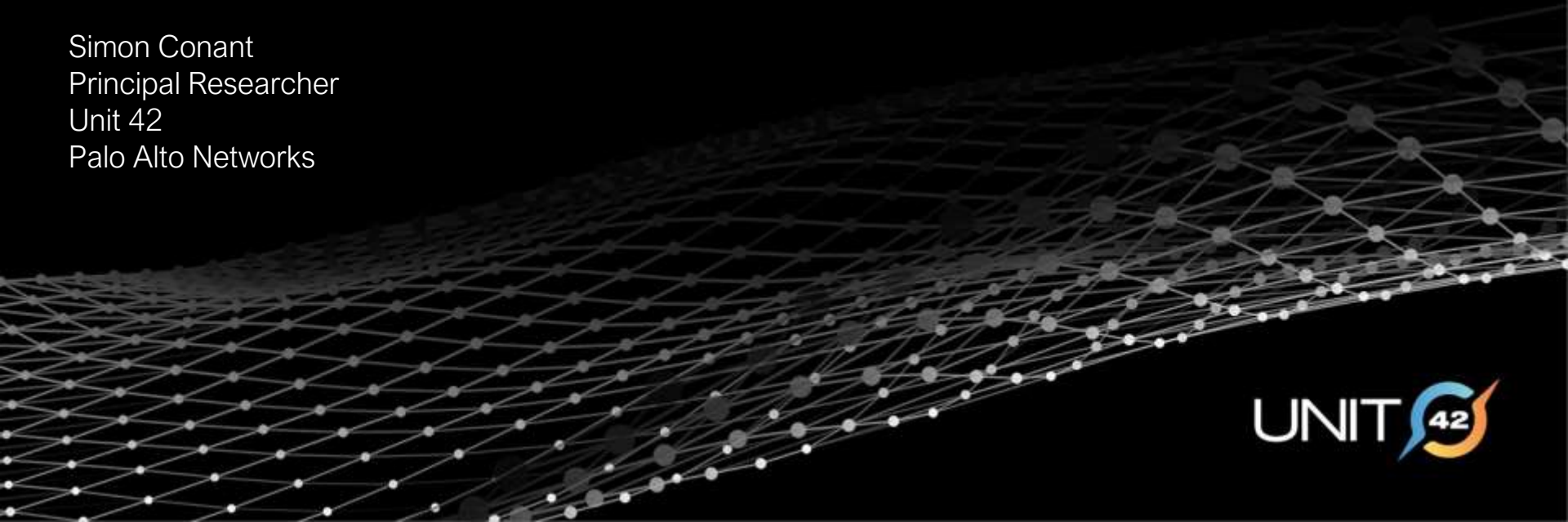
“*Just another day on the Internet*”

Today’s Threat Landscape

Simon Conant
Principal Researcher
Unit 42
Palo Alto Networks



SIMON CONANT | PRINCIPAL RESEARCHER

EXPERTISE IN NATION STATE SPONSORED ACTIVITY, FINANCIALLY-MOTIVATED ATTACKS, MALWARE AND INFRASTRUCTURE ANALYSIS, AND THE UNDERGROUND ECONOMY

OVER A QUARTER CENTURY OF EXPERIENCE INCLUDING NETWORKING, INFRASTRUCTURE, MALWARE ANALYSIS, AND ATTRIBUTION RESEARCH

SEATTLE USA

UNIT 42

Agile team spread across the globe

Average of two new pieces of research a week

Experts in hunting and collection of unknown threats

Experts in complete reverse engineering of malware using code analysis

THREAT INTELLIGENCE

Collection, processing, and storing of adversary and organizational data

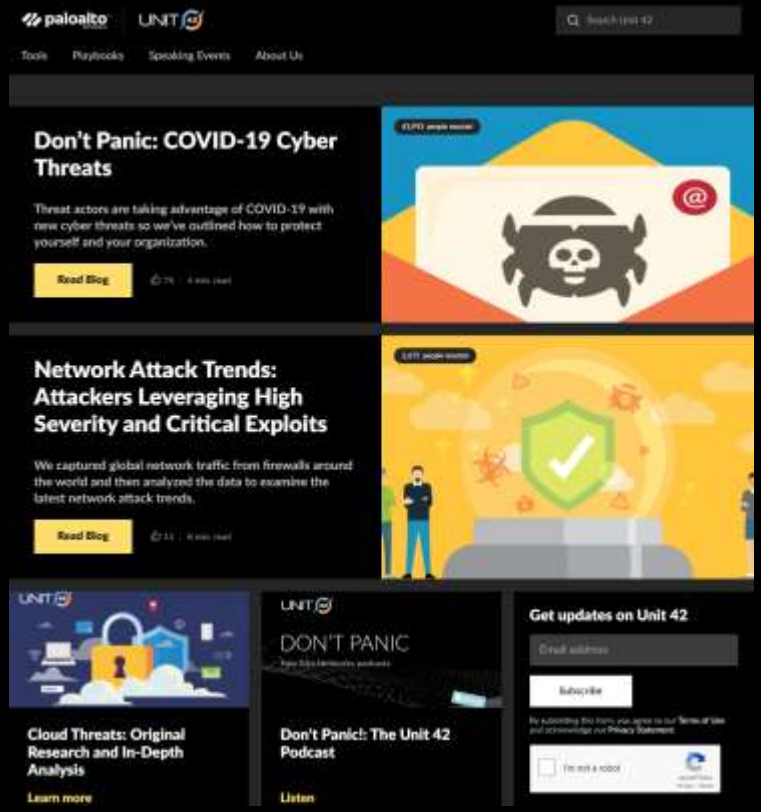
Provide context to threat indicator data to produce assessments relevant to the organization

Understand the adversary

Understand our own environment

Better assess and mitigate risk


COLLECTION
& RESEARCH
PRODUCT
IMPLEMENTATION
INITIAL
DIRECTION
WWW
UNIT 42
ANALYSIS
42
PUBLICATION


paloalto
UNIT 42
Search Unit 42
Tools
Playbooks
Speaking Events
About Us
Don't Panic: COVID-19 Cyber Threats
Threat actors are taking advantage of COVID-19 with new cyber threats so we've outlined how to protect yourself and your organization.
Read Blog
Network Attack Trends: Attackers Leveraging High Severity and Critical Exploits
We captured global network traffic from firewalls around the world and then analyzed the data to examine the latest network attack trends.
Read Blog
Cloud Threats: Original Research and In-Depth Analysis
Learn more
DON'T PANIC
Don't Panic!: The Unit 42 Podcast
Listen
Get updates on Unit 42
Email address
Subscribe
I'm not a robot

YOU ARE A TARGET

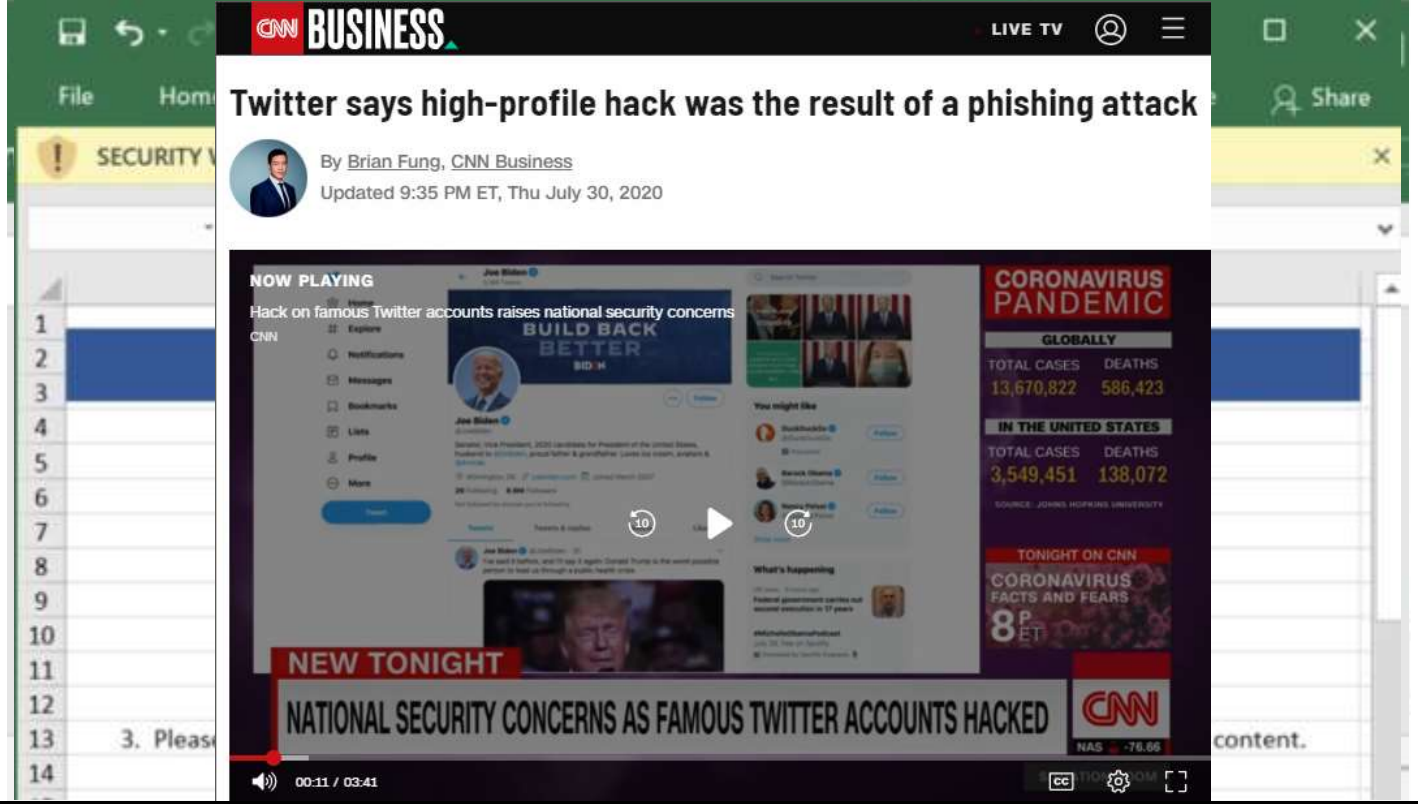
ANYONE CAN POTENTIALLY BE A TARGET DEPENDING ON MOTIVATION AND MISSION

WHO IS THE ADVERSARY?

WHAT ARE THEIR MOTIVATIONS?

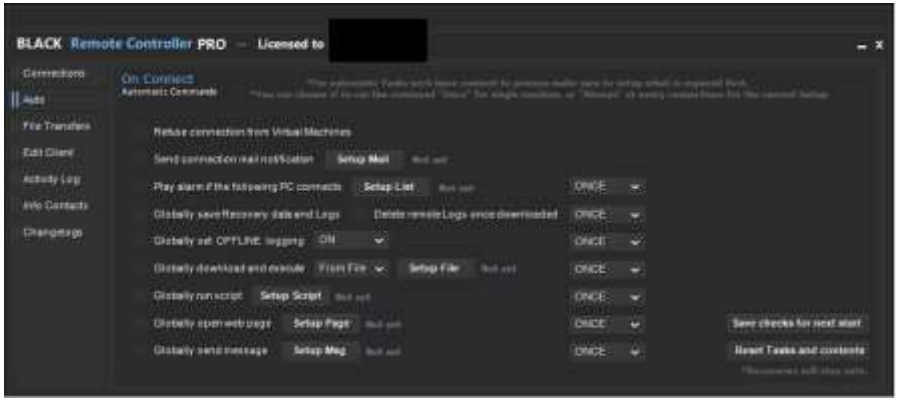
TRENDS

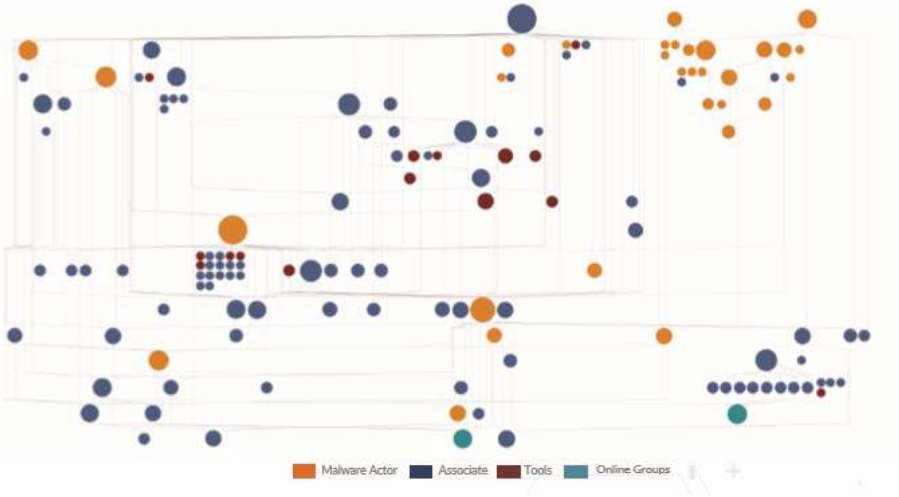
HOW IS THIS THREAT DEVELOPING?



SOCIAL ENGINEERING IS KING

HUMANS CURIOSITY IS THE MOST AVAILABLE VULNERABILITY





WHAT KEEPS ME AWAKE AT NIGHT?

(OR IN A JOB!)

THE NATION STATE ADVERSARY

ASSYMETRIC WARFARE

Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups

September 13, 2019

WASHINGTON – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced sanctions targeting three North Korean state-sponsored malicious cyber groups responsible for North Korea's malicious cyber activity on critical infrastructure. Today's actions identify North Korean hacking groups commonly known within the global cyber security private industry as "Lazarus Group," "Bluenoroff," and "Andariel" as agencies, instrumentalities, or controlled entities of the Government of North Korea pursuant to Executive Order (E.O.) 13722, based on their relationship to the Reconnaissance General Bureau (RGB). Lazarus Group, Bluenoroff, and Andariel are controlled by the U.S.- and United Nations (UN)-designated RGB, which is North Korea's primary intelligence bureau.

"Treasury is taking action against North Korean hacking groups that have been perpetrating cyber attacks to support illicit weapon and missile programs," said Sigal Mandelker, Treasury Under Secretary for Terrorism and Financial Intelligence. "We will continue to enforce existing U.S. and UN sanctions against North Korea and work with the international community to improve cybersecurity of financial networks."

MALICIOUS CYBER ACTIVITY BY LAZARUS GROUP, BLUENOROFF, AND ANDARIEL

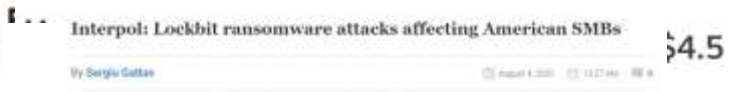
- DPRK
  - Lazarus Group
  - Bluenoroff
  - Andariel
- Sony Pictures Entertainment
- Wan(n)acry(ptor)
- SWIFT attacks
- Targeted financial / disruption / espionage attacks

THE FINANCIALLY-MOTIVATED ACTOR

HOW CAN THEY MAKE A BUCK FROM YOU?

CRYPTOCURRENCY MINING

RISK/REWARD & ROI



07/28/2020 00:47:12

Support

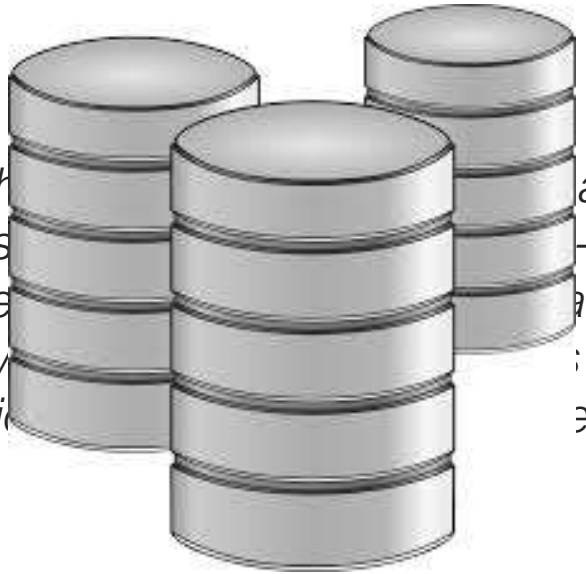
Here are the list of recommendations to avoid such a things in future:

- Turn off local passwords
- Force end of administrators sessions
- In group policy set up wdigest value to "0", If the UseLogonCredential value is set to 0, WDigest will not store credentials in memory.
- Update passwords every month !
- Check the granted privileges for users, to make them maximum reduced privileges and access only to exact applications.
- In most cases there would enough standard windows software like an Applocker.
- Approve to run only necessaries applications ONLY.
- Don't count on the Anti-Virus, there is no one AV that really helps, they can be useful only in long-term infections, if hackers for some reasons didn't attack in short time.
- Install Endpoint Detection and Response security (EDR) and teach the IT-admin to work with it.
- For huge companies we suggest at least 3 system administrators working 24 hours, maximum 4 admins working 3 shifts for 8 hours per day, that would be enough.

RANSOMWARE

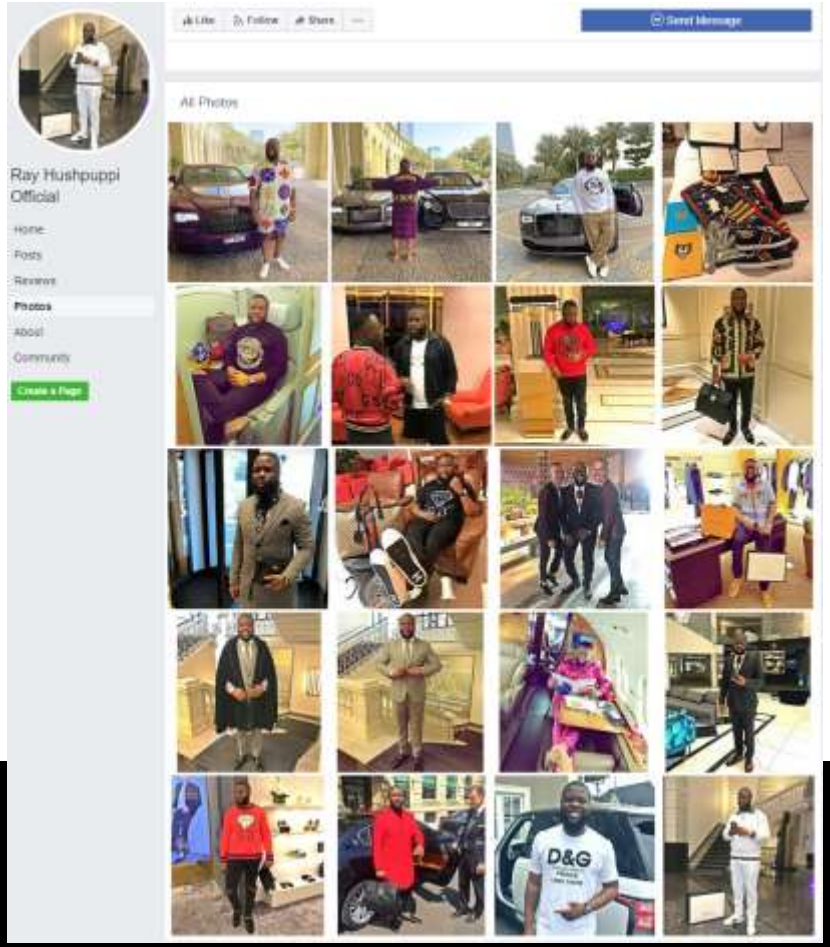
IT'S WHAT I'D DO

- IBM X-Force on Iran:
  - *…"they observed th a text document full of usernames and pas -email accounts"…"they didn't see any evide able to bypass two-factor authentication, how s secured with any second form of authenticati ed on to the next one on their list."*



DATA

…IS MONEY


Like
Follow
Share
Send Message
Ray Hushpuppi Official
Home
Posts
Reviews
Photos
About
Community
Create a Page
All Photos
D&G

THE HACKTIVIST

STEPPING BEYOND GRAFFITI

THE INTERNET OF THINGS

THE INTERSECTION OF CONVENIENCE AND SECURITY

BBC Sign in News Sport Reel Worklife Travel Future

NEWS

Home US Election Coronavirus Video World US & Canada UK Business Tech

Technology

New Zealand stock exchange halted by cyber-attack

5 hours ago Share

The New Zealand stock exchange was knocked offline two days in a row due to a cyber-attack.

NZX said it had first been hit by a distributed denial of service (DDoS) attack from abroad, on Tuesday

The exchange said the attack had "impacted NZX network connectivity" and it had decided to halt trading in cash markets just before 16:00 local time

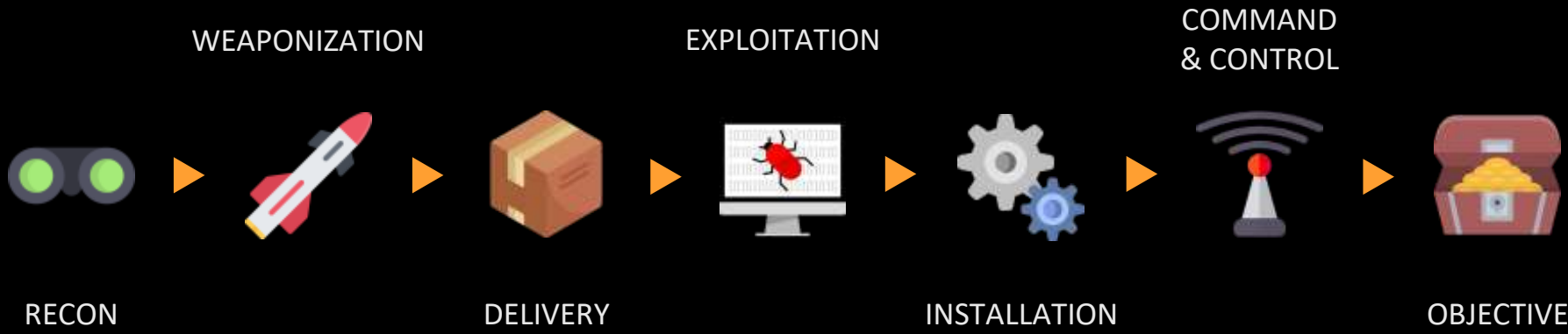
Trading halted briefly for a second time, on Wednesday, but was back up and running before the end of the day

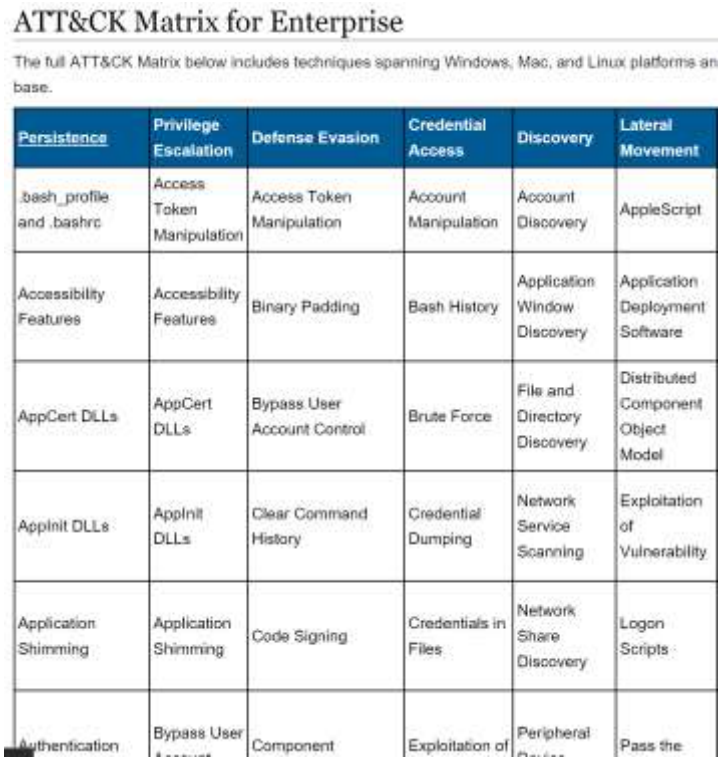
COMMODITY MALWARE

ENABLING THE LEAST-SOPHISTICATED CYBERCRIMINAL

RESPONSE

ATTACK LIFE CYCLE





ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms an
base.

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software
AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Distributed Component Object Model
AppInit DLLs	AppInit DLLs	Clear Command History	Credential Dumping	Network Service Scanning	Exploitation of Vulnerability
Application Shimming	Application Shimming	Code Signing	Credentials in Files	Network Share Discovery	Logon Scripts
Authentication	Bypass User	Component	Exploitation of	Peripheral	Pass the

LOOKING AT THREATS DIFFERENTLY

UNDERSTANDING THE WHOLE THREAT, NOT JUST PIECES

WE ARE THE CYBER THREAT ALLIANCE

AlienVault · Check Point · Cisco · Dragos · Eleven Paths · Fortinet · Intsights · Juniper · K7 Computing · lastline · McAfee · NEC · NETSCOUT | Arbor · NTT · paloalto · panda · radware · Rapid7 · Reversing Labs · Scitum · SecureBrain · SK infosec · SonicWall · Sophos · Symantec · verizon

AN EXISTENTIAL THREAT

THE WORST COULD VERY WELL HAPPEN

SONY PICTURES ENTERTAINMENT

ALREADY FORGOT THIS LESSON?

INFORMATION SECURITY IS NOT OPTIONAL

RISK MATCHED WITH APPROPRIATE COUNTERMEASURE

HOW WOULD YOU ATTACK YOU?

HOW WOULD YOU STOP IT?

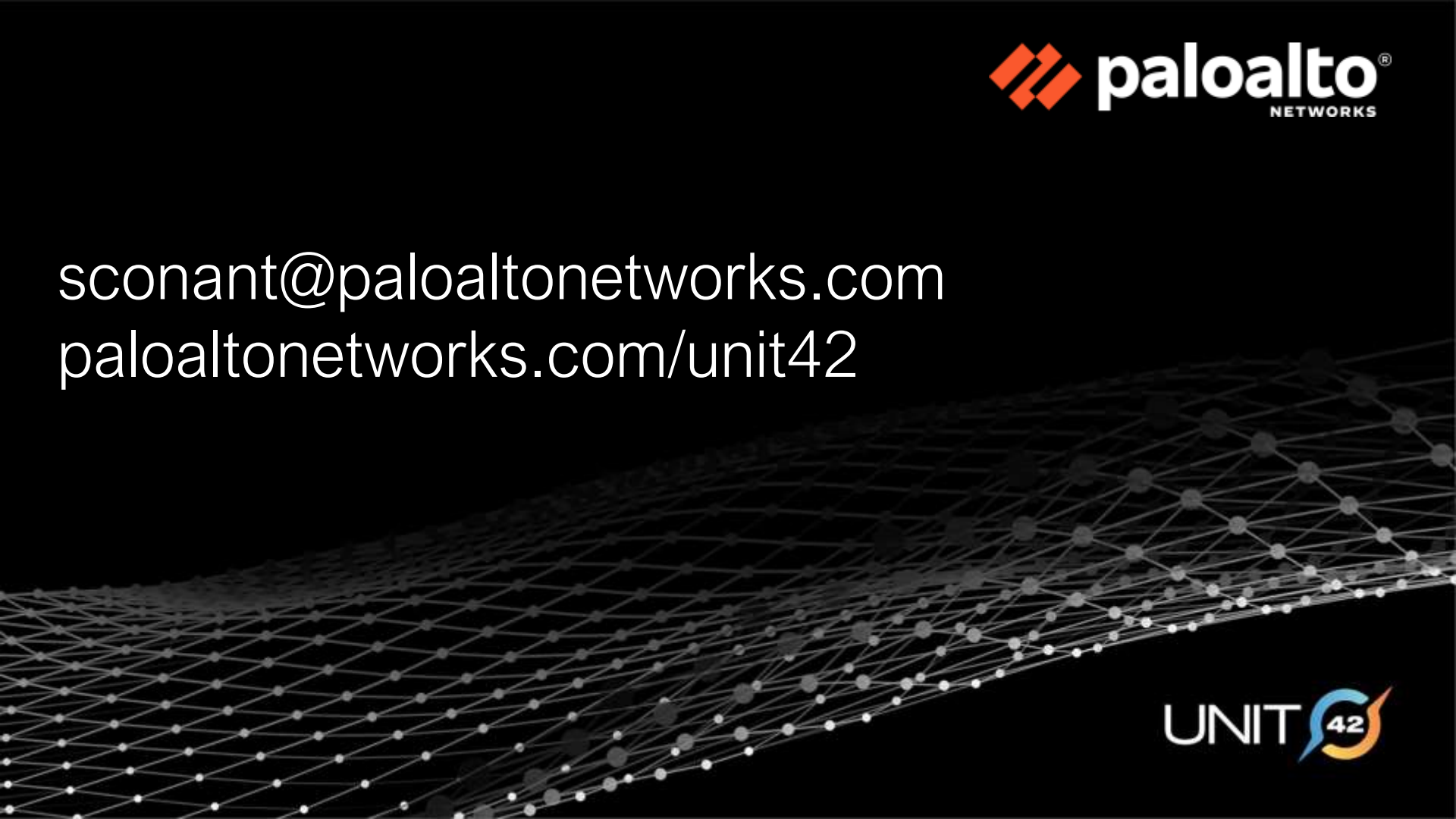
'Just another day on the internet'

Leading security researcher Troy Hunt told the BBC the company appeared to handle the breach well.

“In many ways, this is just another day on the internet: a large online asset suffers a data breach and millions of usernames and passwords get leaked,” he said.

“JUST ANOTHER DAY ON THE INTERNET”

WHAT IS YOUR ROLE IN IT?


paloalto
NETWORKS
sconant@paloaltonetworks.com
paloaltonetworks.com/unit42
UNIT 42