Are you Ransom Ready?

Current Cyber Threats & Challenges

SWISS GRC DAY 2022

4 Mai 2022

Building a better working world

Cyber Threats | Ransomware as a concrete example

Ransomware trends

Capitalizing on attractive events

For example COVID, political events, ecological disasters etc.

Coordination with other malware

A devastating combination: Emotet – TrickBot - Ryuk

Exfiltration of sensitive data (CID, PII, business critical information)

Exfiltration before encryption

Collaboration between ransomware groups

Maze confirmed that they have established an alliance with LockBit and founded a cyber syndicate

Ransomware | Setting the Scene

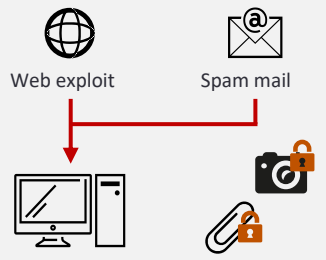
What is ransomware?

Ransomware isn't new – over the last five years the number of attacks has grown tremendously, usually with financially motivated cyber criminals extorting relatively small amounts of money from victims whose data they are holding hostage (encrypted).

Ransomware is a sophisticated threat that affects the organization's or individual user's data to extort money locking the entire system or holding specific files hostage.

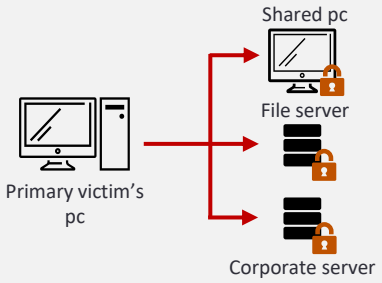
Different types of ransomware impact

Encryption of corporate and personal documents and data



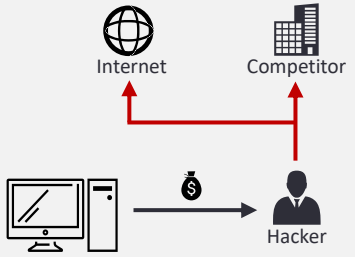
Ransomware is introduced via routes including email and web, and encrypts corporate/personal documents/data.

Secondary and tertiary **damage** (encryption of file servers)



File servers / shared PCs are exposed to secondary/tertiary damage via network drives and other vulnerabilities etc.

Disclosure of information during restoration attempts



Confidential documents could get leaked via covert communication channels.

The Evolution of Modern Ransomware*

- **2021**
- **2020**
  - Rise of Double Extortion
- **2019**
  - BGH targets state and local governments
- **2018**
  - Emergence of Big Game hunting (BGH)
- **2017**
  - Nation-state sponsored WannaCry and NotPetya combine worm-like techniques to spread worldwide
- **2016**
- **2015**
  - Over 4 million ransomware samples
  - Ransomware-as- a-service appears
- **2014**
  - CryptoLocker appears
  - RSA encryption keys
- **2013**
- **2010**
  - 10,000 ransomware samples
  - Birth of Bitcoin
  - Screen-locking ransomware appears
- **2009**
  - Malware evolves from pushing rogue antivirus (AV) to encrypting files
- **2008**
- **2006**
- **2005**
  - First variants of modern ransomware appear in the wild

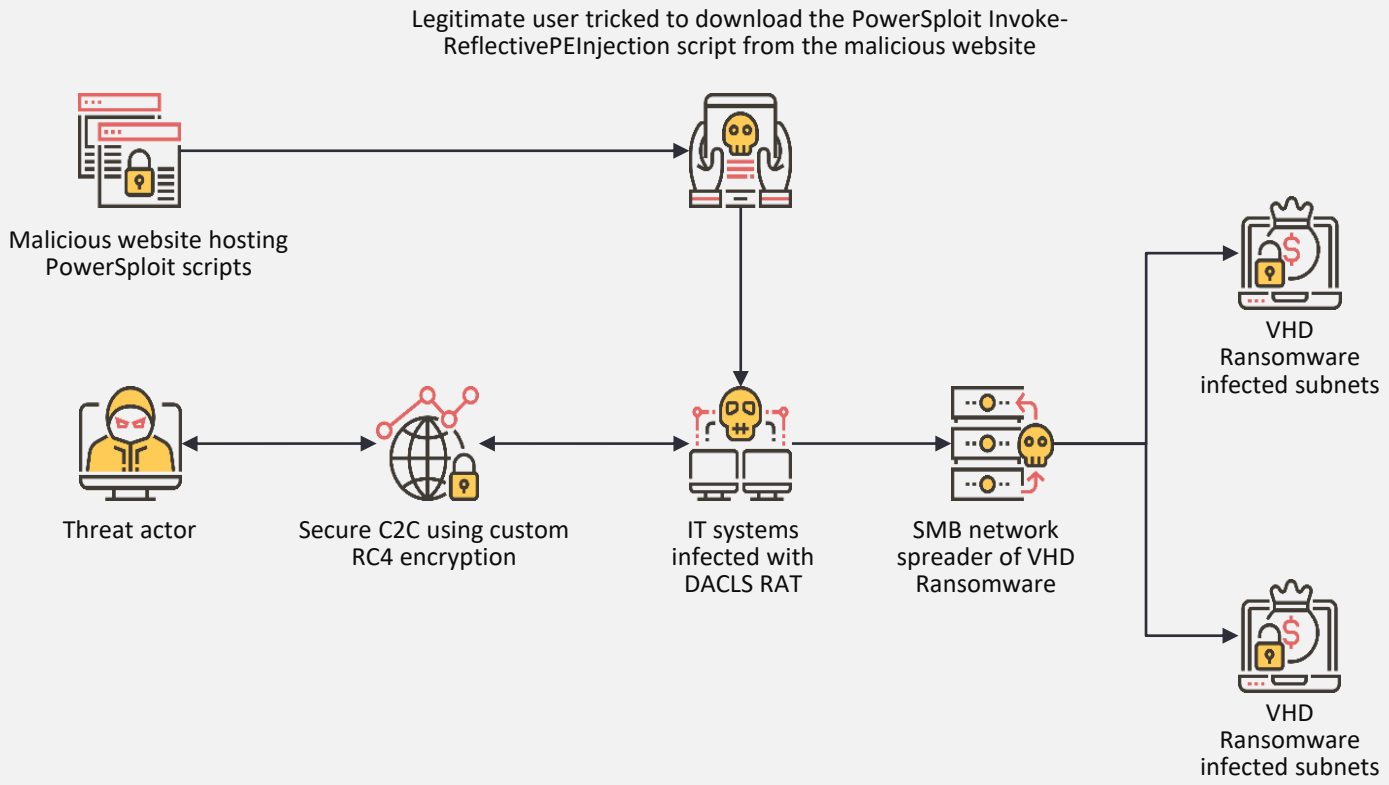
[*] Crowdstrike Whitepaper "Evolution of Ransomware" 2020 – updated by EY

Ransomware | Rise of Big Game Ransomware

Big Game Ransomware

- Starting with the summer of 2018 organized threat actors shifted their focus from large scale indiscriminate ransomware attacks to targeted attacks against high value targets
- The shift created a cybercrime ecosystem around “big game” ransomware which provides ransomware operators with services like:
  - Bulletproof hosting
  - Initial access to targets
  - Money laundering services
  - State sponsored actors adopted the same TTPs for sabotage or financial gain
- Ransomware groups have adopted ‘Double Extortion’ techniques. Threating to leak stolen data to increase pressure and rate of success.

Lazarus APT (North Korea) deploying DACLS (MATA Framework) and VHD ransomware against a global organization

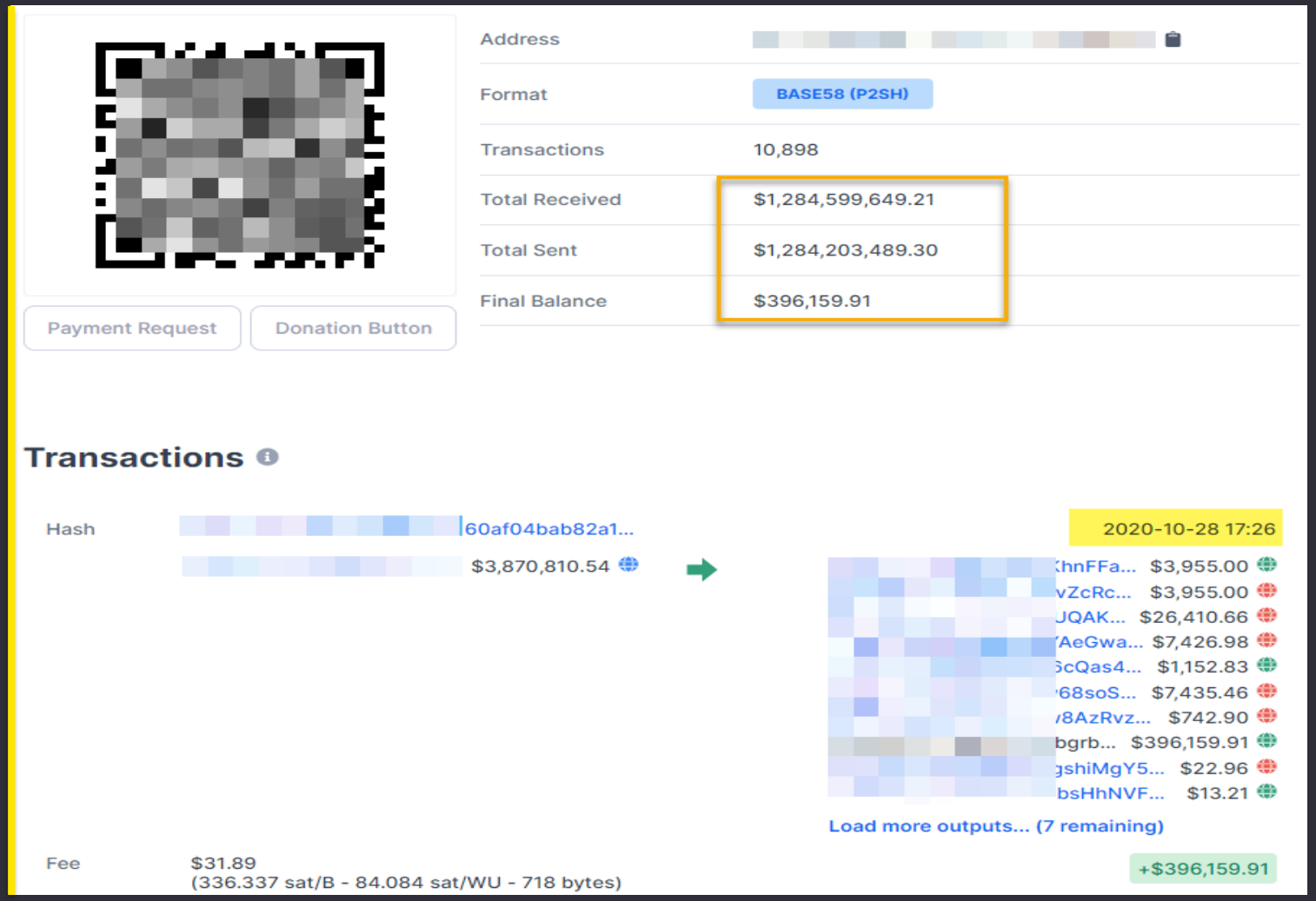


Source: EY

Ransomware | Rise of Big Game Ransomware

Revenues

- Based on several data sources it is estimated that the big game ransomware groups generated up to 20bn USD in revenue in 2020, as compared to 11bn USD in 2019
- Ryuk ransomware group generated over time around 1,3bn USD



Ransomware | Rise of Big Game Ransomware

Revenues

- Based on several data sources it is estimated that the big game ransomware groups generated up to 20bn USD in revenue in 2020, as compared to 11bn USD in 2019
- Ryuk ransomware group generated over time around 1,3bn USD
- Based on our research REvil/Sodinokibi earned an estimate of 90,6mil USD in October 2020 alone

REvil/Sodin Extension		Ransom in USD
61lwu8	$	250,000.00
hc772z62	$	7,000,000.00
u8zzfx05	$	25,000.00
8ofbn5t	$	25,000.00
knw6herb9	$	25,000.00
gg5a8	$	5,000.00
928zr40t83	$	7,500,000.00
035i588g	$	4,000,000.00
3r974v	$	280,000.00
d60xvis7h	$	20,000.00
001715yzkz	$	4,000,000.00
44p72	$	25,000.00
h617x752	$	25,000.00
6219wo	$	25,000.00
25li8ph	$	25,000.00
3ywz4	$	25,000.00
7w4k1518xa	$	50,000.00
o94q7v0h	$	25,000.00
ylbg83p65o	$	25,000.00
o1d4v6u2v	$	25,000.00
i1bi0z	$	200,000.00
67k5c9k	$	25,000.00
g3lm9r616n	$	25,000.00
3o2z0vv	$	4,000,000.00
1yj227r	$	60,000,000.00
mttu9	$	3,000,000.00
Ransom Requests in October 2020	$	90,630,000.00

Ransomware | The Summer of 2021

What's new in the World of Ransomware

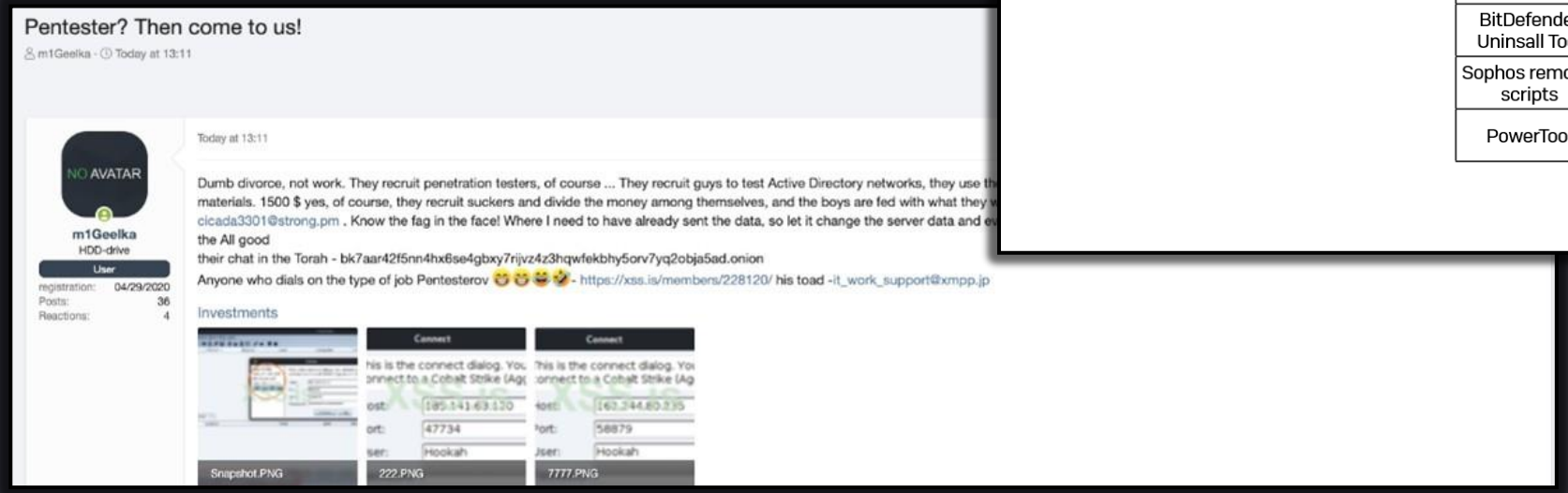
- **August 2021 –** Disgruntled ransomware affiliate leaks the Conti gang's affiliate manual.
  - Claims to be 'ripped off' by the Conti Gang
  - One of the first to leverage new exchange 'Proxy Shell' weakness
  - Manual contains step-by-step guides, tooling, anti-virus evasion techniques and credential stealing software.

Conti Ransomware Tools

Initial Access	Execution	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Exploit FortiGate Firewall	PowerShell scripts	PowerUp	Process Hacker	Mimikatz	Routerscan	psexec	Conti Ransomware
Spearphishing attachment	psexec	SharpUp	Gpedit.msc	Invoke-Kerberoast	Adfind	wmic	rclone
ProxyShell exploit	wmic	BeRoot	Set-Mp Preference	wmic NTDS.dit dump	nltest	Atera	Data exfiltration to Mega.io
	Metasploit	PrivEsc	Gmer	wmic LSASS dump	Windows net commands	Anydesk	
	Cobalt Strike	FullPowers	PCHunter	Metasploit	netscan	Splashtop	
			TrendMicro Remover	Cobalt Strike	SharpView	Remote Utilities	
			BitDefender Uninsall Tool		PowerViewer	Invoke-SMBAutoBrute	
			Sophos removal scripts		Invoke-UserHunter	CVE-2021-34527	
			PowerTool		Metasploit	CVE-2017-0144	

sophoslabs

Source: Sophos labs



Source: mcafee, link

The Ransomware attack journey | 5 Stages

1 Initial Access & Delivery

- **Exploitation of public-facing assets**
- Third-party compromise & abuse of trusted access
- Purchased access & malware delivery services
- Insider Threat, Affiliate programs offering big rewards

2 Persistence, Internal Recon, & Lateral Movement

- **Native Windows tools & services (e.g., PSExec, MSHTA, RunDLL32, schtasks)**
- OFFSEC tools (e.g. Cobalt Strike, PowerSploit)
- Nearby vuln exploitation (e.g., ETERNALBLUE)
- Modified admin tools (e.g., AdFind, ADRecon)

3 Privilege Escalation & Defense Evasion

- Antivirus process-killing
- Legitimate process injection (e.g., explorer)
- **Priv Escalation tools (e.g., Mimikatz, Bloodhound)**
- LPE vuln exploitation (e.g., Zerologon)
- Local Security Authority secrets dumping

4 Data Exfil & Ransomware Impact

- Backup server access
- **Shadow copy deletion**
- Encrypted or proxied C2 (e.g., anonymous VPNs, Tor, self-signed certs)
- Simultaneous domain-wide deployment (via Domain Controllers, update servers, etc.)

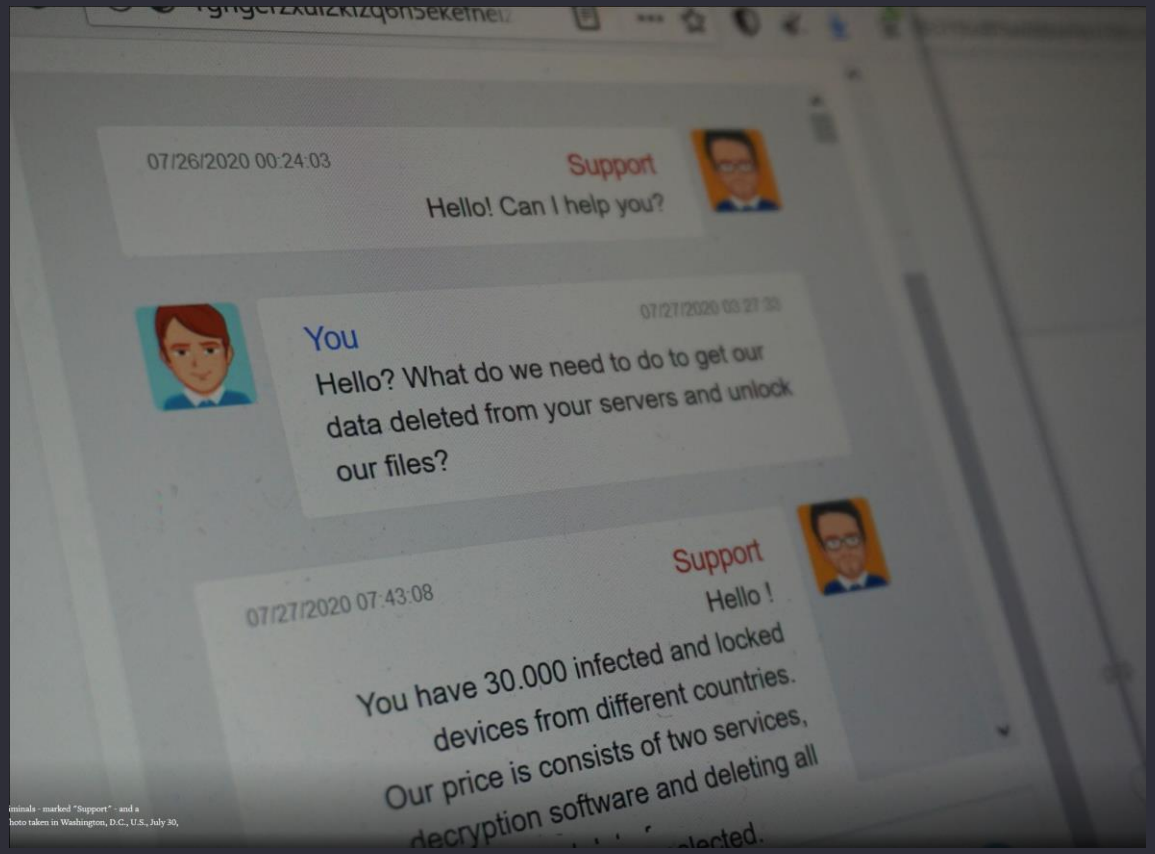
5 Extortion & Negotiation

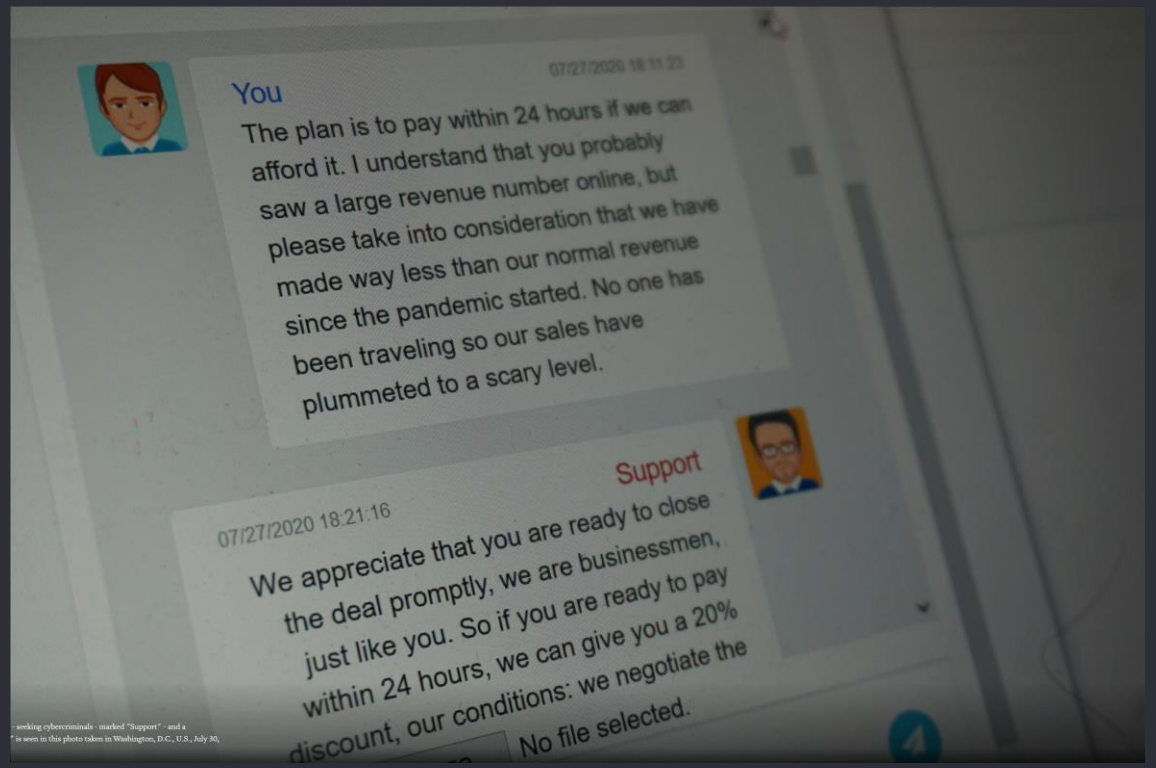
- Pricing model dependent on encrypted devices, victim revenue, & contents of stolen data
- Payment in common & custom cryptocurrencies
- **Staggered disclosure of stolen data**
- Discount decryption as proof of "good faith"

Focus Areas	Endpoint Security & Awareness	IT Change Management	Privileged Access Management	Data Protection and Secure DR	Business Impact Assessment

EY

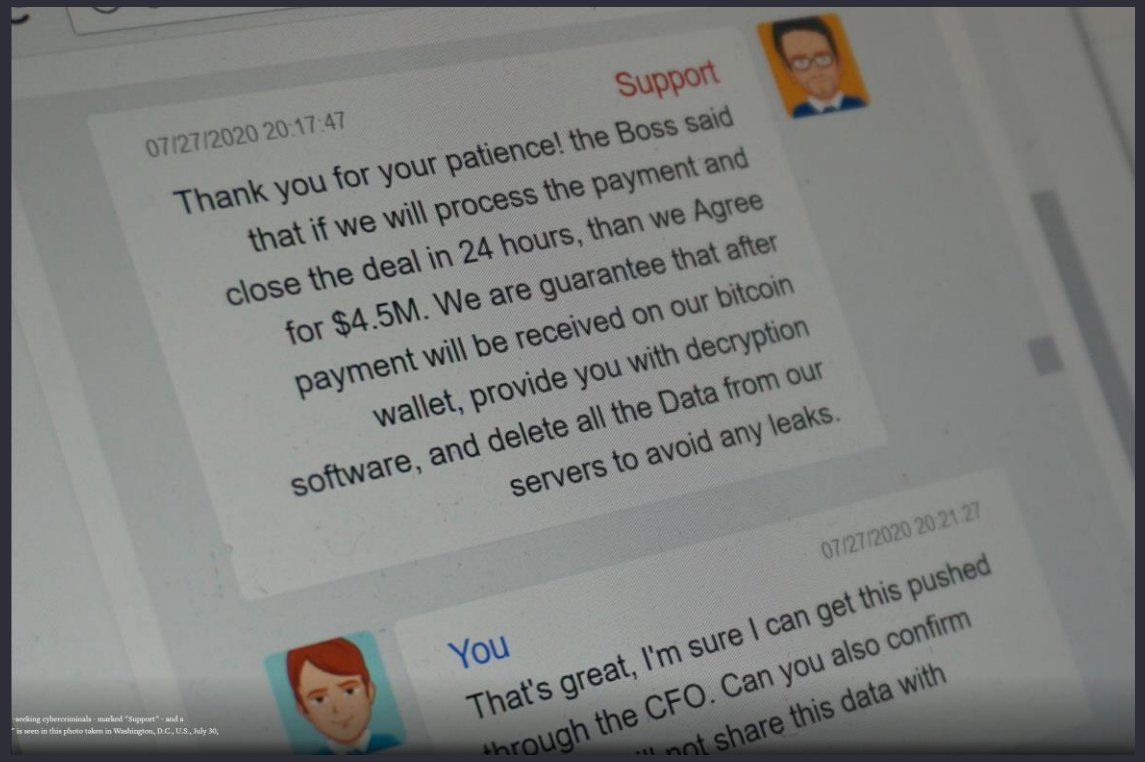
The Ransomware Support Hotline | Negotiation with the attacker

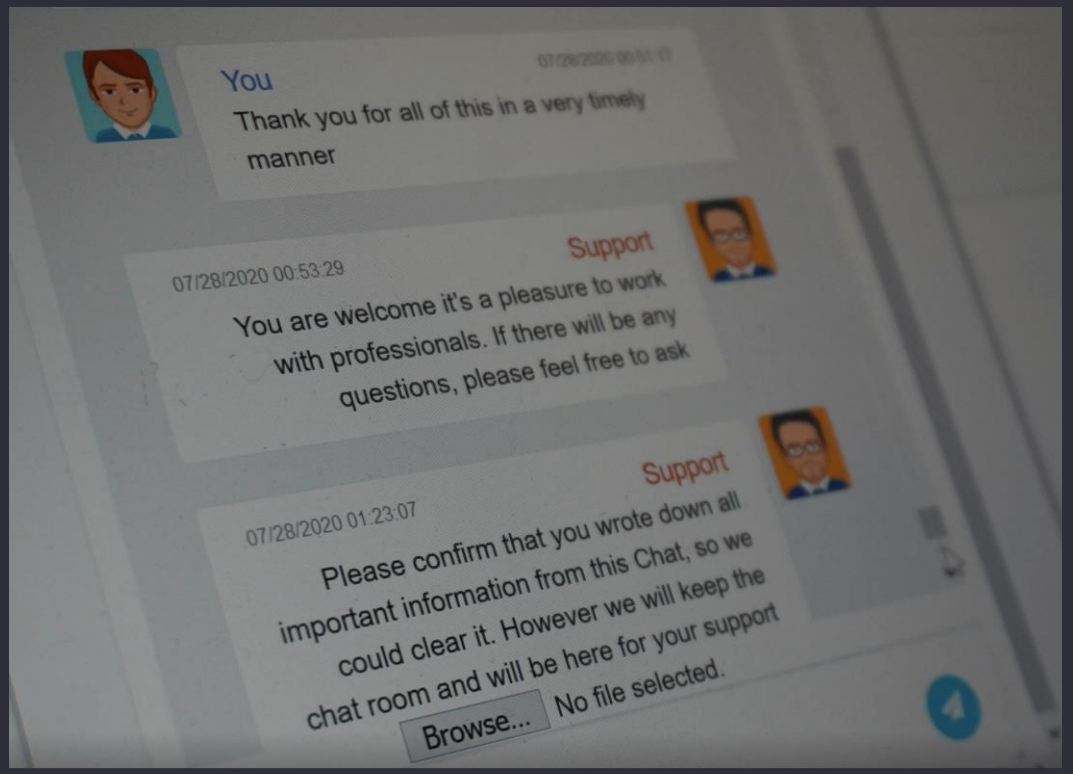




Source: https://www.reuters.com/article/us-cyber-cwt-ransom-idUSKCN24W25W

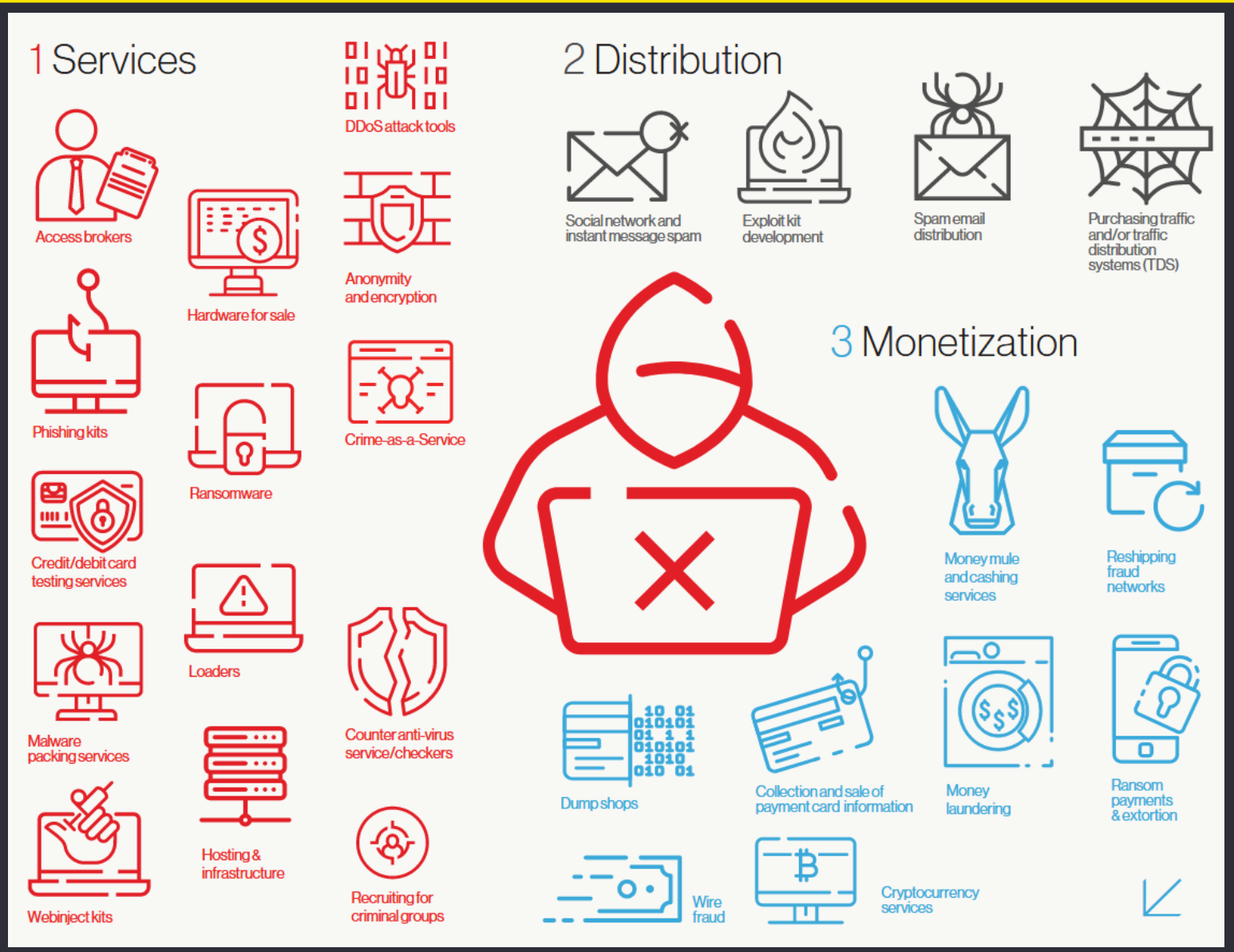
The Ransomware Support Hotline | Negotiation with the attacker





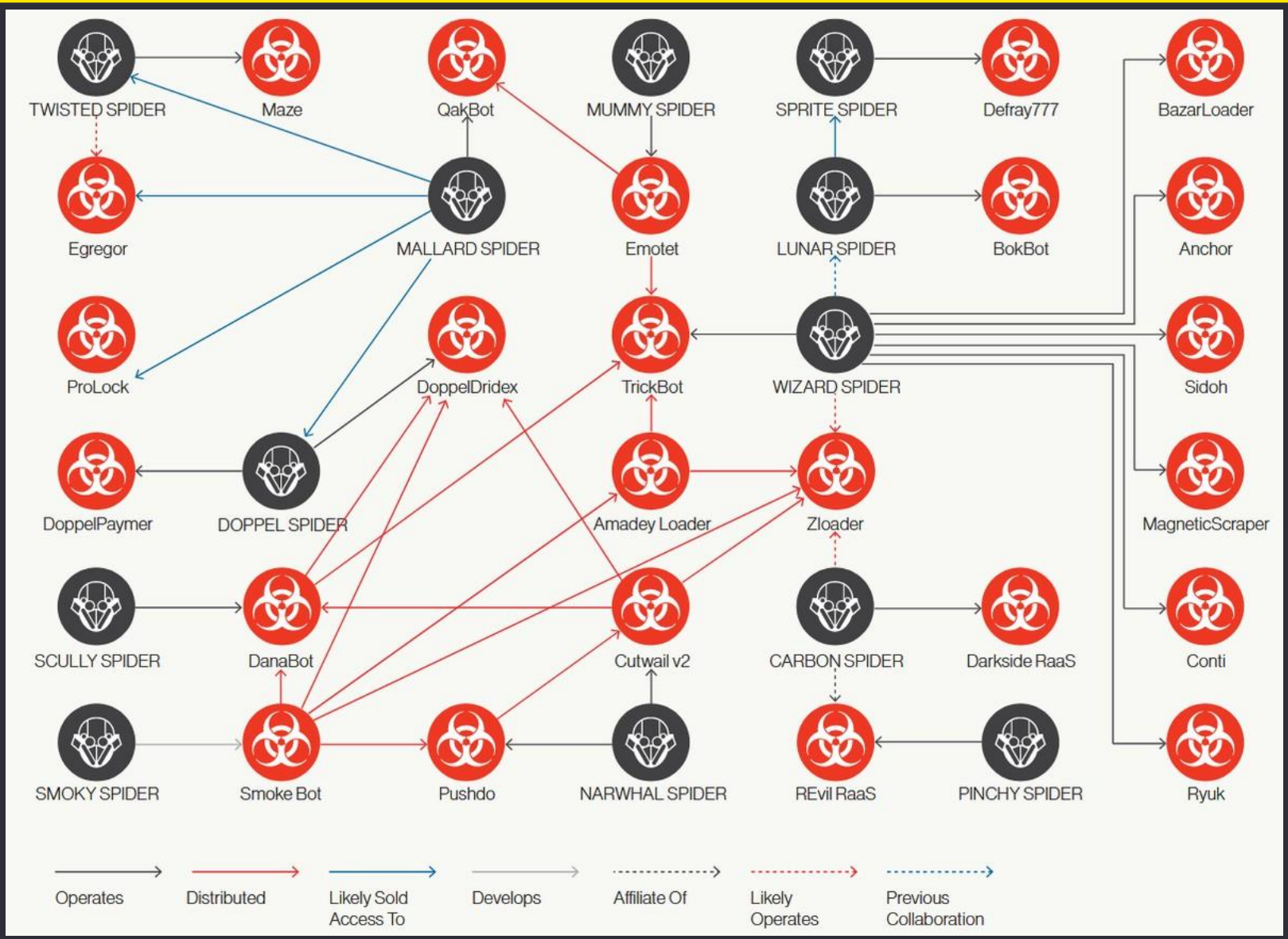
Source: https://www.reuters.com/article/us-cyber-cwt-ransom-idUSKCN24W25W

Cybercrime | Big Business and division of work



Source: CrowdStrike (https://rootdaemon.com/2021/02/25/this-chart-shows-the-connections-between-cybercrime-groups)

Cybercrime | Groups and their collaboration



Source: CrowdStrike (https://rootdaemon.com/2021/02/25/this-chart-shows-the-connections-between-cybercrime-groups)

Cyber Threat Resilience | Tactics & Techniques & Measures

	Initial Access & Delivery	Persistence, Internal Recon, & Lateral Movement	Privilege Escalation & Defense Evasion	Data Exfil & Ransomware Impact	Extortion & Negotiation
Tactics & Techniques	• Exploitation of public-facing servers/services • Credential-stuffing • Third-party compromise & use of trusted access • Purchased access & malware delivery services • Widespread exploitation of public-facing vulnerabilities	• Local account creation • Offensive security/post-exploitation tools • Native Windows tools & services • Local/nearby vulnerability exploitation • Basic command-line tools • Open-source administration tools	• lsass dumping • Offensive security/open-source tools • Windows Defender tampering & file exclusion • A/V process-killing • Local Security Authority secrets dumping • Legitimate process injection • Signed malicious binaries	• Backup server access • Shadow copy deletion • Widespread process-killing to “unlock” files • Encrypted/proxied C2 • File transfers to actor-controlled servers • Domain-wide deployment via Domain Controllers	• Price based on number/types of encrypted devices, victim revenue, & contents of stolen data • Common & custom cryptocurrencies • Price spikes based on countdowns and other factors • Staggered disclosure of stolen data • Discounted/free decryption as proof of “good faith”
Identify	• Attack surface reduction • Asset discovery	• Role/asset mapping • Enterprise network map	• Privileged access management • Privileged tool inventory	• Backup access logging • AD forest mapping	• Create response playbooks • Escrow & crypto wallets
Protect	• Proactive cred management • Patch/vuln management	• Network segmentation • Restricted Gold Loads	• Privileged app restriction • Group Policy enforcement	• Trust relationship limits • Data encryption at-rest	• Establish criteria for payment/negotiation
Detect	• IAM logging/alerting • Perimeter device logging	• Role-based endpoint alerting • Scheduled admin activity	• Process metadata alerting • Binary signature validation	• Backup health monitoring • JA3 fingerprint detection	• Actor comms playbooks • Dark web/leak monitoring
Respond	• Attack path analysis • Central access revocation	• Real-time endpoint isolation • Rapid subnet isolation	• Endpoint image capture • Process tree logging	• Rapid backup disconnect • DC trust revocation	• Stolen data classification • LE/IR data-sharing
Recover	• DMZ asset reimaging • Centralized access management	• Backup validation • Gold Load reimaging	• Federated cred revocation • Attack timeline generation	• Offline backup restoration • Data access identification	• Legal impact assessment • Cyber insurance liaison

EY

Questions ?

Building a better working world

Appendix

Cyber Threat Resilience | Ransomware attacks

Organizations across sectors face severe risks from ransomware attacks

Categories of Ransomware Actors

Sophisticated criminal groups are conducting opportunistic manual intrusions across sectors

- Professional groups have operated for multiple years, garnering hundreds of millions in ransoms
- Multiple specialists that collaborate on different phases of the operation

New actors continually emerge and disappear, often using poorly implemented variants

- Encryption is a wildcard; files could be impossible to decrypt, free to decrypt, or not actually impacted
- Mix of open-source tools and customized malware that evades proactive blocks
- Deals are unreliable; ransoms could be stolen & data could be re-ransomed, leaked, or sold

State-sponsored actors continue to invest in disruptive & destructive capabilities that could be activated at any time

- Self-propagation via widespread, "wormable" vulnerabilities
- May see "false flag" ransom demands, limiting response options

Noteworthy Incidents

September 2020: ~400 Universal Health Systems locations impacted by Ryuk ransomware; recovery took three weeks

Est. Impact: $67 million

May 2020: REvil group auctions data stolen from GSMLaw after initial $21 million ransom refused

Est. Impact: $42 million

April 2020: Maze ransomware disrupted telework and other systems at Cognizant; clients pause projects in response

Est. Impact: $60 million

June 2017: Merck impacted by Russian GRU's destructive malware, NotPetya (disguised as ransomware)

Est. Impact: $1.3 billion

Attack Trends

- Compromise of trusted third parties to gain initial access
- Malware delivery services and purchase of remote access from intrusion specialists
- "Living-off-the-land" techniques to evade detection and controls
- Compromising legitimate accounts for persistence
- Rapid intrusions intentionally timed for weekends and low-staffing periods
- Data theft & threats of disclosure ("multiple ransoms")
- Consistent & resilient market for Ransomware-as-a-Service

EY

Kontaktangaben des Präsentators Tom Schmidt

Kontakt:

+41 58 286 64 77

+41 79 558 42 08

tom.schmidt@ch.ey.com

Follow and connect with Tom on:
LinkedIn | XING | Twitter

Hintergrund und Erfahrung:

- Tom Schmidt ist Partner bei EY im EMEIA Financial Services Consulting mit Fokus auf Cybersecurity, Cyber Risk Management, Information Security und IT Risk Consulting bei zahlreichen Finanzdienstleistern und Industriekunden. Er hat mehr als 30 Jahre Erfahrung im Bereich Information Technology und mehr als 20 Jahre praktische Information Security / Cybersecurity und Cyber Risk Management Erfahrung
- Tom Schmidt ist der Cybersecurity & Cyber Risk Management Leader FSO Schweiz und EMEIA FSO Cybersecurity Competency Leader
- Er hat grosse Erfahrung in der Leitung und Durchführung von Cybersecurity Assessments, Cybersecurity Consulting Projekten, IT Security Audits, IT und Cyber Risk Management Projekten, Drittpartei-Risiko Management (Third Party Risk Management – TPRM) sowie generischen IT Audit- und IT Consulting-Dienstleistungen für nationale und internationale Finanzdienstleistungs- und Industriekunden
- Tom Schmidt ist Betriebsökonom HWV/FH und Master of Advanced Studies (MAS) Information Security
- Er ist Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC) und Certified ISO 27001 und ISO 22301 Lead Implementer
- Des weiteren ist Tom Schmidt Fachrat und Dozent am MAS Cyber Security, Hochschule Luzern

EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com/be.

EY is a leader in serving the financial services industry
We understand the importance of asking great questions. It's how you innovate, transform and achieve a better working world. One that benefits our clients, our people and our communities. Finance fuels our lives. No other sector can touch so many people or shape so many futures. That's why globally we employ 26,000 people who focus on financial services and nothing else. Our connected financial services teams are dedicated to providing assurance, tax, transaction and advisory services to the banking and capital markets, insurance, and wealth and asset management sectors. It's our global connectivity and local knowledge that ensures we deliver the insights and quality services to help build trust and confidence in the capital markets and in economies the world over. By connecting people with the right mix of knowledge and insight, we are able to ask great questions. The better the question. The better the answer. The better the world works.

ey.com/fs