RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART1-W09**

Multifaceted Extortion: Insider Look at Ransom Payments and Cyber Defense

Dave Wong

Vice President, Consulting
Mandiant

Nick Bennett

Vice President, Consulting
Mandiant

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Agenda

- Multifaceted Extortion and Ransomware Attack Trends
- Extortion Payment Trends
- Lessons Learned: Case Study in Effective Cyber Defense

Legal Disclaimer

Case studies and examples are drawn from our experiences and activities working for a variety of customers, and do not represent our work for any one customer or set of customers. In many cases, facts have been changed to obscure the identity of our customers and individuals associated with our customers.

Ransomware By The Numbers

INVESTIGATION TYPE	GLOBAL	AMERICAS	EMEA	APAC
Ransomware Investigations	23% (-2%)	22% (-5.5%)	17% (-5%)	38% (+25.5%)

	GLOBAL (DAYS)	AMERICAS (DAYS)	EMEA (DAYS)	APAC (DAYS)
All	21 (-3)	17 (0)	48 (-18)	21 (-55)
Ransomware	5 (0)	4 (+1)	4	9
Non-Ransomware	36 (-9)	32	60	38

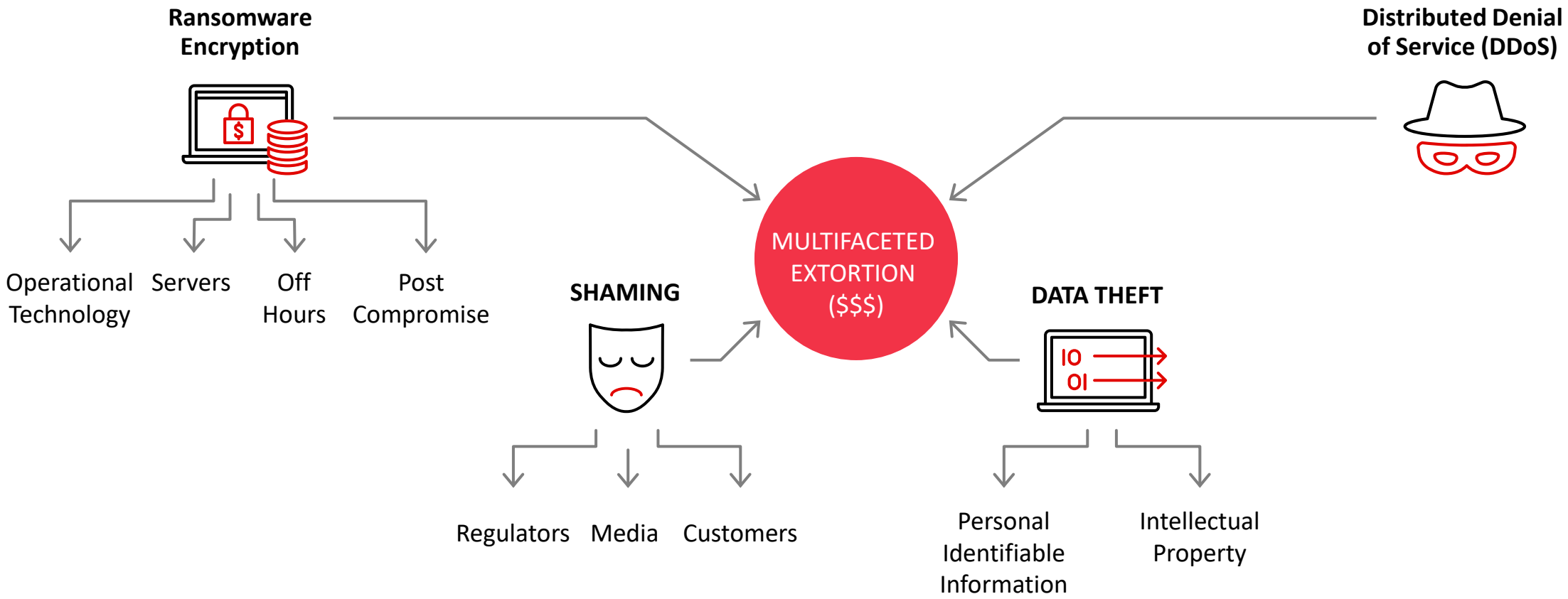
Mandiant (2022). M-Trends 2022.

Ransomware – Attacker Tools and Techniques

MALWARE FAMILY	PERCENTAGE OF RANSOMWARE INTRUSTIONS BEGINNING 2022
LOCKBIT	20%
AVOSLOCKER	12%
ALPHV/BlackCat	8%
HIVELOCKER	8%
Other (<5% Each)	52%

INITIAL ATTACK VECTOR (WHEN KNOWN)	PERCENTAGE OF RANSOMWARE INTRUSTIONS BEGINNING 2022
Prior Compromise	35%
FAKEUPDATES Malware	30%
Exploits	22%
Stolen / Guessed Credentials	13%

Extortion Accelerators – Multifaceted Extortion



Ransomware Payment Trends

- 69% increase in ransomware losses YOY per FBI
- $602 Million in Cryptocurrency Paid to threat actors in 2021*

CYBERSECURITY

Senate report reveals gaps in data collection on ransomware payments

BY INES KAGUBARE - 05/24/22 5:07 PM ET

*2022 Crypto Crime Report by Chainanalysis: https://go.chainalysis.com/2022-crypto-crime-report.html

Payment Recovery

- Payments have been recovered with the assistance of law enforcement
- Many victims are concerned about retaliation
- Over 98% of Mandiant clients that pay, do not attempt to recovery funds

RSAConference2022

Case Study

Two Victims, Two Outcomes

Both Victims Suffer Attack

- Initial access to workstations
- Lateral movement and install backdoors
- Sells access & hand off to another threat actor
- Internal reconnaissance & data theft
- Lateral movement to privileged systems
- Credentials obtained for account in domain admins group

Lessons Learned

- Ransomware detection is about the whole attacker lifecycle
- Importance of early detection
- Detection is not just a tooling problem

The Response Begins

The Incident

- Initiate Enterprise-Wide Investigations
- Intel Tells Us:
  - Ransomware Deployment Imminent
  - Victim 1 notifies law enforcement
- Begin Remediation Workstream
  - Gain Control
  - Rapid Field Assessments
  - Prepare for Recovery

Lessons Learned

- Attacker intelligence dramatically changes our response

Containment Considerations – Isolation

Victim 1

- Victim confirms all remote access requires MFA
- Playbook in place to shutdown egress traffic
- Victim stages control to block egress

Victim 2

- Victim has multiple remote access mechanisms – not all protected with MFA
- Research needed to execute egress blocking

Lessons Learned

- Validation of assumptions / attack surface management
- Importance of comprehensive visibility
- Preparation and playbooks for breach response

Rapid Field Assessments

Victim 1

- Limited security architecture weaknesses
- Victim executed plan to gain control of privileged accounts

Victim 2

- Significant technical weaknesses in on-prem identity
- Victim engaged in extended cat and mouse game with attacker

Lessons Learned

- Strong security architecture begets strong cyber defense
- Documented ownership and authority facilitates fast action
- Importance of human expertise

Crisis Management & Communications

Victim 1

- Prepared holding statements for employees & customers in advance
- Had experts lined up to negotiate with threat actor

Victim 2

- Management waivered on whether they should contact the threat actor, causing attack to escalate
- Information from incident leaked and customers jumped to inaccurate conclusions

Lessons Learned

- Plan for the worst
- Communications is key
- Ransomware is not just an IT or CISO problem

The Attacker Strikes – Encryption

Victim 1

- Alert triggers on failed ransomware deployment
- Playbook to block egress – ends attacker access
- Investigation and eradication complete while egress down

Victim 2

- Attacker begins deploying encryptors to enterprise
- Victim unable to control attacker access
- Victim begins to shutdown servers
- Unknown number of machines encrypted

Lessons Learned

- Visibility and strong security architecture provide decision-making confidence

Extortion and Recovery

Victim 2

- Victim can’t bring some critical applications back online without decryptor
  - Decryptor clumsy and doesn’t scale
- Fear of encrypting resuming as systems brought back online
- Victim pays ransom to avoid release of stolen data, stop attack, and help with recovery

Key Takeaways

- Build a robust security program, but prepare for successful attacks
- Effective cyber defense not just about latest tools – but about intelligence, expertise, and execution
- Strong security architecture begets strong cyber defense
- Multi-faceted extortion increases pressure to pay ransoms

RSAConference2022

Thank You