Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Streaming Edition 2021

ASTREA Advanced Security, Training Research, Events Agency

Atelier tecnologico

Il Ransomware è una minaccia per il business. Scopri se la tua organizzazione è resiliente

Angelo Perniola, Senior Strategic Consultant, FireEye Mandiant

Gabriele Zanoni, Senior Strategic Consultant, FireEye Mandiant

16 Marzo 2021 orario 11:20-12:00 - StreamingEdition

#securitysummit #streamingedition

Angelo Perniola

SENIOR STRATEGIC CONSULTANT – MANDIANT

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT
Streaming Edition
16-17-18 marzo 2021

FIREEYE™ | MANDIANT®

Gabriele Zanoni

SENIOR STRATEGIC CONSULTANT – MANDIANT

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT
Streaming Edition
16-17-18 marzo 2021

FIREEYE™ | MANDIANT®

Mandiant Security Consulting

Prevent, detect and respond to advanced cyber security events and protect your organization's critical assets.

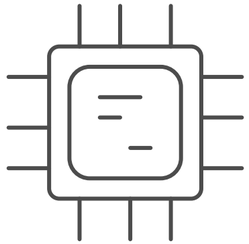
77%

Trusted by organizations worldwide – **Over 77%** of Fortune 100 companies[1]

Cutting-edge **threat intelligence** informed by frontline adversary exposure

15+

15+ years responding to and remediating headline breaches



Cyber security services enabled by **purpose-built technology**

Mandiant DNA – Pioneers in sophisticated incident response

Global workforce of over 300 consultants in 20+ countries

Portfolio of services to **assess, enhance and transform** security posture and upskill internal security staff

Industry-recognized LEADER

- 2019 Forrester Wave: Cybersecurity IR
- 2018 Forrester Wave: External Threat Intel
- 2018 IDC: U.S. Incident Readiness, Response and Resiliency
- 2018 IDC: Asia Pacific Threat Lifecycle Services

The FireEye Mandiant Ecosystem

Agenda

- Threat Landscape
- Ransomware Exploitation Model
- Key Protection Recommendations
- Ransomware and Cyber Extortion
- Q&A

Let’s Get Started!

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.

Threat Landscape

Ransomware – Where it Began

- Has evolved in its long history
- Bad Admins / Time and or Logic Bombs
- Mix of Corp and Individual Targets
- OP TOVAR (2014) & AVALANCHE (2016)

- **Ransomware is malicious software that denies access or holds data hostage**
- **The definition will change over the years and over this presentation**

Enter The APT

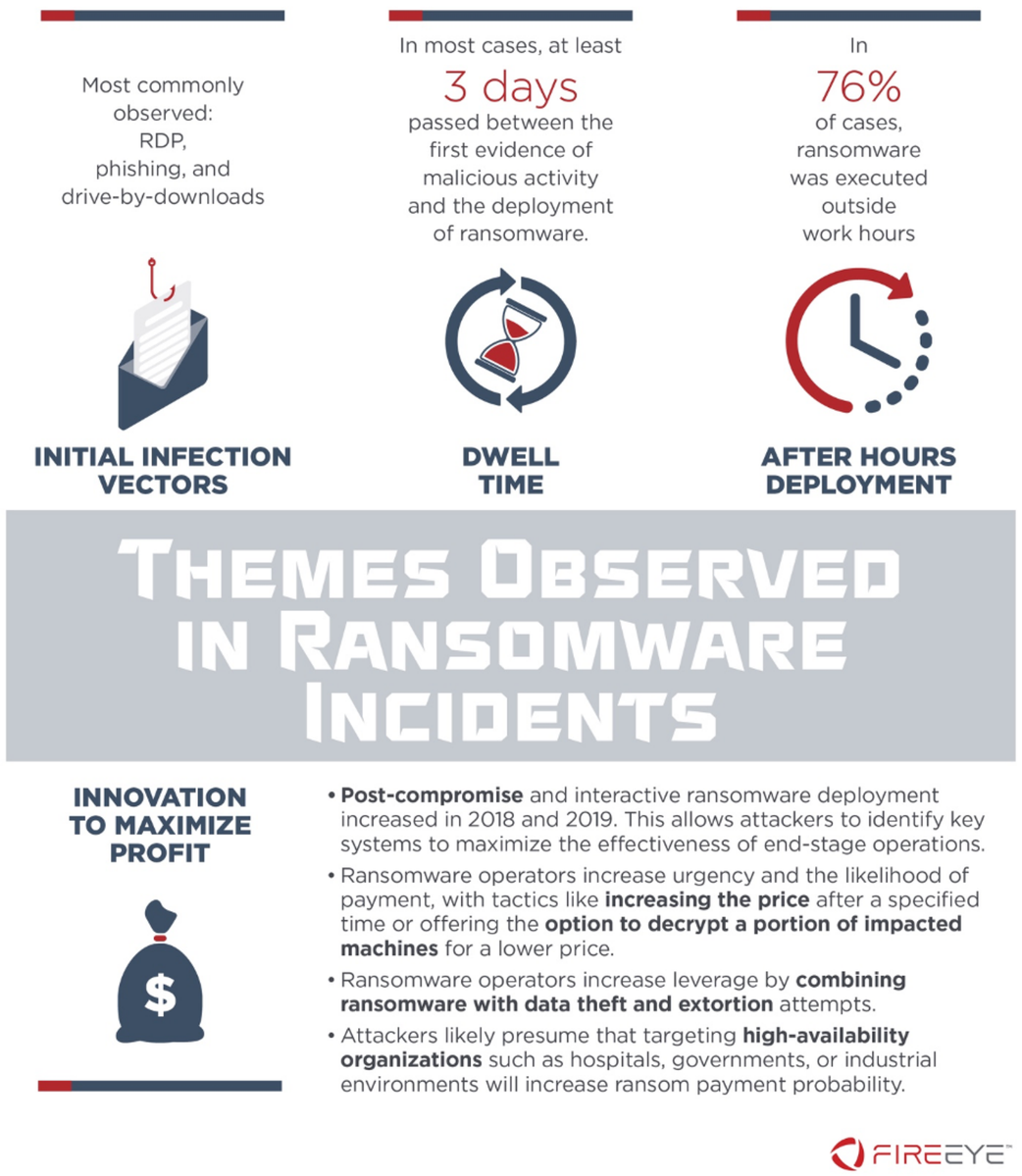
- Mid 2010 APT Threat Actors Destructive Attacks
- Likely North Korea & Russia (or Anti-Ukranian) attribution for to serve different purposes.
- ETERNAL BLUE
- Shadow Brokers
- Third Party Issues?

- **Wannacry**
- **Not Petya**
- **Hugely Disruptive and largely not targeted**
- **Impact possibly less than Media Reporting in Most Cases**

Streaming Edition

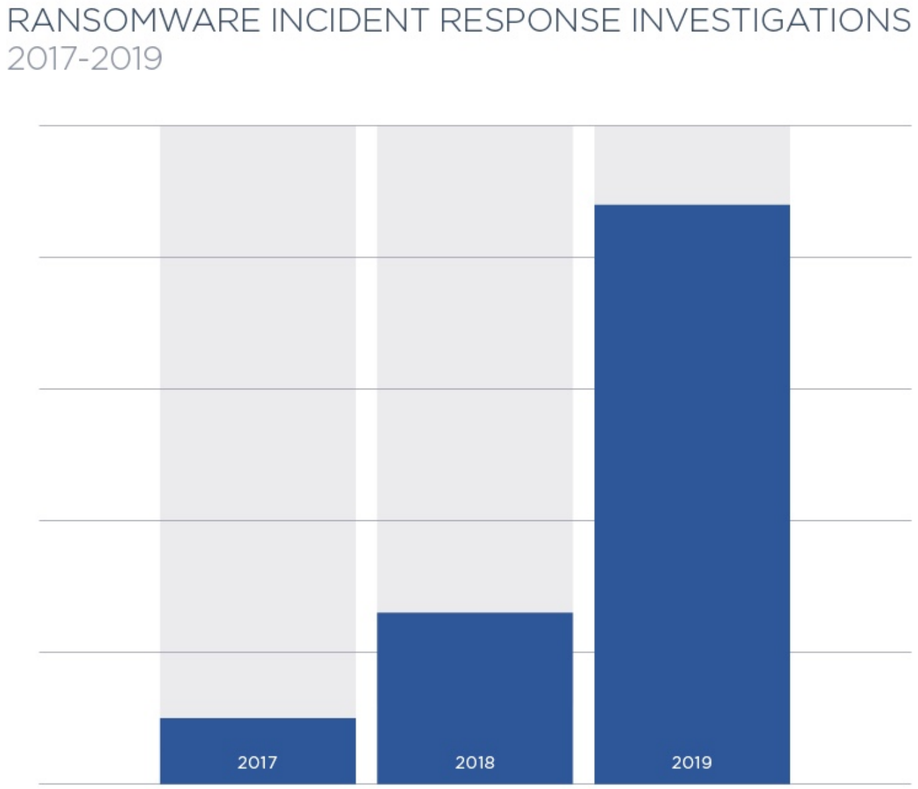
Organized Crime

- SamSam
  - M.O change
  - Targeted cities and Municipal authorities
  - Iranians Indicted
- GandCrab
  - $2b in 15 months
  - Developers claim to have made $150m

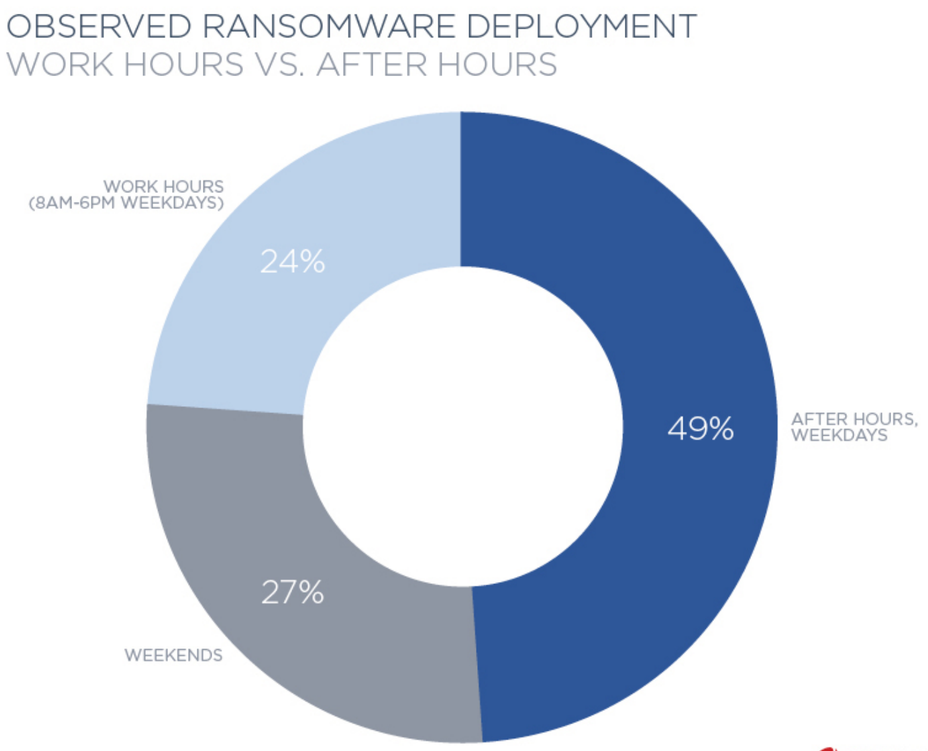


More Cybercriminals Turn To Ransomware

Ransomware investigations have increased over 700% since 2017



76% of Ransomware attacks occur after hours



Where Are We Today

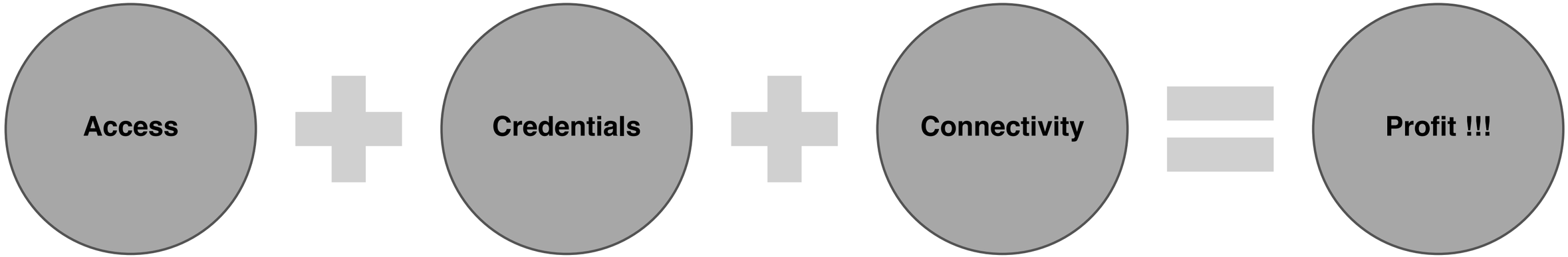
- RaaS both
  - Targeted, Profiled, Tailored, Hand Delivered and aimed at high value targets
  - Lower value targets still being extorted
- Evolution – It's an ongoing process
- Sodinokibi, Maze, RYUK, Phobos, Netwalker
- Encrypt, Exfiltrate, Sell, Public Shaming

- **Growing business**
- **Targeting varied and extensive**
- **Copycats are following the trend**
- **Ability to Outsource everything**

Streaming Edition

Ransomware Exploitation Model

Ransomware Exploitation Model



How is Access Obtained?

Common Vectors	Methods	Examples
External Facing Systems (+ limited segmentation between DMZ and internal systems)	Vulnerability Exploitation	Remote Code Execution (RCE) Vulnerabilities in **deployed technologies** (e.g., CVE-2019-11510, CVE-2019-1978, CVE-2020-0609, CVE-2020-0610) Vulnerabilities in **third-party hosted applications** (e.g., WordPress, WebLogic)
	Access using legitimate credentials • Brute Forcing • Simple password guessing • Previous phishing campaigns • Credentials purchased in an underground marketplace	External-facing systems with Remote Desktop Protocol (**RDP**) enabled from the Internet **Single-factor VPN**, Citrix, or other remote access technologies
Phishing Emails	Delivery of emails that contain either embedded links to malicious websites or weaponized attachments	**Malicious attachment** that relies upon macros to download Trickbot malware Malicious website which masquerades as a legitimate site to capture credentials for access via **single-factor external facing systems**
Drive-by-download	**Compromised web infrastructure** used to deliver multistage malware to facilitate follow-on activity	Ransomware infections traced back to a **user in the victim environment navigating to a compromised website** that resulted in a DRIDEX infection

How are Credentials Obtained?

- After initial endpoint exploitation – an attacker will attempt to obtain credentials that are resident in memory or on disk
- **Example method that can be used to extract passwords from disk:**
  - Dump the registry hives to extract and crack password hashes for local accounts, cached domain credentials, and service accounts
  - “Pass-the-hash” (no cracking) for password hashes for local accounts
- **Example credential dumping tools that can extract passwords and hashes from memory:**
  - Mimikatz
  - ProcDump
  - Windows Task Manager

How are Credentials Obtained? (cont.)

- Requesting Kerberos tickets for service accounts – and attempting to crack the password from the service ticket
  - No administrative access to an endpoint required

- Via clear-text passwords – either on disk or in memory
  - Configuration files or passwords stored in a file on the endpoint
  - Group Policy Preferences
  - Legacy settings that result in clear-text passwords being stored in memory

How is Connectivity Exploited?

- With the correct credentials, default Windows protocols allow for remote connectivity amongst systems.
- Placement of backdoors on endpoints – for beaconing and persistent access to an environment
- Common Windows protocols that are used for lateral movement:
  - SMB
  - RDP
  - WMI

- Common methods that are used for lateral movement and ransomware deployment:
  - PsExec – free remote administration tool that uses SMB for connectivity
  - RDP – attacker remotely logs onto an endpoint for pivoting, staging, or deployment of malware
  - Scripts that leverage SMB or WMI connectivity - for remote deployment of malicious files to endpoints

POLL #1

«Alla luce di quanto appena visto, considero la mia organizzazione adeguatamente protetta contro attacchi Ransomware?»

Key Protection Recommendations

Access Protections – External-Facing Systems

- Scan, identify, and mitigate weaknesses in external-facing systems and applications (vulnerability and patch management)
- Segment external-facing systems (e.g., DMZ) from internal systems and applications
- Harden access methods for external-facing systems
  - Multi-factor authentication
  - Network Level Authentication for RDP
  - Restrict inbound access where possible
  - Disable legacy and vulnerable protocols from being accessible from the Internet

Access Protections – Phishing

- Disable macros (external senders) and harden MS Office
- Remove local administrative permissions for standard users
- Use separate (non-privileged) accounts for daily usage (including when accessing email and external resources)
- Patch systems and third-party applications (e.g., Java, Adobe)
- Disable legacy protocols (e.g., SMB v1.0, PowerShell v2.0)

Credential Protections

- Minimize privileged credential exposure
  - E.g., harden systems so that privileged and/or service accounts cannot be used for logons to standard endpoints
- Remove the capability for local administrative accounts to be used for remote logons to other endpoints
- Randomize the password for built-in local administrative account on endpoints
- Harden endpoints so that clear-text passwords are not stored in memory

Connectivity Protections

- Restrict system-to-system communications (i.e., Windows Firewall, Network Segmentation)
- Restrict egress access, ports, and protocols
- Remove the capability for privileged accounts to be used for remote logon purposes
- Disable unnecessary services on endpoints
- Leverage dedicated privileged access workstations (PAWs) for performing administrative tasks

Key Recommendations

- Endpoint Hardening
- Network Segmentation
- Reducing the exposure of privileged credentials
- Controlling how privileged accounts can be used
- Tested backup and recovery processes

- Mandiant Whitepaper:

  “Ransomware Protection and Containment Strategies”

  https://www.fireeye.com/blog/threat-research/2019/09/ransomware-protection-and-containment-strategies.html

Ransomware and Cyber Extortion

Ransomware and Cyber Extortion

Ransomware

- *"A **malicious software** that is **designed to deny access to data** by encrypting them with a key known only to the attacker"*
- Prevents you from accessing your data

Cyber Extortion

- *"The act of **using, or threatening to use, force to obtain money**, services, or something else of value from a victim"*
- Threatens to make your data known to others

POLL #2

«Pagare o non pagare?

Sono in grado di rispondere a questa domanda?»

Streaming Edition

Payment Considerations

- Multiple plausible scenarios depending on whether the organization decides to pay ransom or not

- **Pay**
  - Data can be returned and/or recovered
  - Data may not be returned
  - Alternative Outcomes
    - Follow-up ransom demands
    - Negotiations
    - Partial payments

- **Don't Pay**
  - No Negative Consequences
    - Adequate backups
  - Prolonged Restoration and Recovery
  - Extortion
    - Threats to go public with stolen information

Streaming Edition

To Pay or Not to Pay?

- Commonly considered factors when deciding on payment of ransom:
  - Human life threat
  - Legal concerns
  - Impact on customers or employees
  - Business impact on the organization
  - Cost of recovery vs. cost of payment
  - Reputational concerns
  - Potential impact of payment of ransom for future ransomware

To Pay or Not to Pay? (cont.)

- Start from a **Ransomware Policy**
  - Default position vs. ransom requests (i.e., “pay” or “don’t pay”)
  - Ransomware-focused Risk Assessment to determine if there is reason to deviate from default position
    - Risk (e.g., Regulatory and Legal, People, Financial, Information, Physical)
    - Decision Owner (e.g., Chief Legal Officer, Chief Risk Officer, CEO, CISO)
    - Risk Rating (output of assessment)
    - Conclusion (“default” or “deviate”)
  - Communication (internal and external)

Key Questions to Ask

Ransomware

How quickly can we **recover our systems and data?**

How **credible is the threat actor?**

Will paying the threat actor **enable us to recover more quickly?**

Will cybersecurity insurance **cover the claim?**

Extortion

Does the threat actor **have access to our data?**

Will the actor escalate their attack and **disrupt our business operations?**

Does the threat actor have **access to our network?**

Can we stall the actor by **paying in small installments?**

How Can FireEye Mandiant Help?

Am I at risk?

How do I prepare for an attack?

Where are my security gaps?

I've been breached. How do I respond?

Q&A

Angelo.Perniola@mandiant.com

Gabriele.Zanoni@mandiant.com

Vieni a trovarci al nostro Stand Virtuale!