Surviving a Ransomware Attack

The Ransomware Situation
Keeping up with the Ransomwares
Case Studies
Lessons from the Field

Lessons from the Field
“By failing to prepare, you prepare to fail.”

Benjamin Franklin
and what every CISO should be saying
**Wilfred Farias**

Wilfred is a cyber-risk manager at Deloitte. He supports the Cyber Incident Response (CIR) team in Toronto, and provides Incident Management and SME support to clients undergoing cyber security incidents.

Wilfred also leads the proactive advisory services, including process and procedure development, technical playbook design, simulation and testing, post-incident reviews, as well as, training and awareness.

---

**Thomas Poinsignon-Clavel**

Thomas is a cyber-risk consultant with a focus on SIEM and IR, combining both a business and a technical profile to be leveraged on mandates ranging from strategic advisory to malware analysis. Thomas has been an incident responder to several major ransomware incidents in varying industries such as healthcare and aerospace, he thereby acquired hands-on expertise in incident remediation & recovery within high-stakes environment.

Thomas also regularly works with Deloitte clients to help them prepare for attacks by setting the proper governance & processes surrounding incident response.
The Ransomware Situation
Ransomware in numbers

- Avg. ransom payment of $50,000
- A new business targeted every 40 seconds
- Above 50% ransomware infections originate from Remote Connections (RDP) compromise
- 98% of ransom payments use Bitcoin
- 40% of Canadian companies opted to pay the ransom...
- Data recovery rate of 80%
Ransomware Costs

**Average cost of ransomware recovery***

$713,000

+ additional costs

---

Impact Factors

- Technical Investigation and Recovery
- Customer Notification and post-breach Protection
- Ransom Payments and Lost of Data
- Regulatory Compliance
- Public Relations
- Attorney Fees & litigation
- Cyber Security Improvements
- Loss of Intellectual Property
- Increased Cost to Raise Debts
- Impact of Operational Disruption or Destruction
- Lost Value of Customer Relationships
- Value of Lost Contract Revenue
- Devaluation of Trade Name

---

Above the surface
Better known cyber incident costs

Beneath the surface
Hidden or less visible costs

---

* Kaspersky Lab
Lasting damage

Average downtime:
10 days

The struggles of evaluating recovery costs against the ransom

Recovery stretches over years

Incident triage efforts comprise <10% of total impact

Impact management

Incident triage

Year 1

Business recovery

2
3
4
5

INACCIDENT TIMELINE

Weeks or months
- Repair damage to the business
- Redesign processes and assets
- Invest in cyber programs to emerge stronger

Days or weeks
- Stop compromises in progress
- Remediate security controls
- Communicate with customers, partners, and other external parties
- Address disruption and business continuity issues

Months or years
Keeping up with the Ransomwares
Evolution of Ransomware

Ransomware prevalence within malware (2015-2018)

Less attacks but higher infection success rates

Ransomwares have upgrades too

Spear-phishing & ransomware, an upcoming duo

RaaS aka commoditized cyber crime

2019 onwards

Mobile ransomware

Cloud ransomware

Internet of Things

AI-based malware

Continuous evasion improvements

- Modular ransomware
- Sleepers
- Fileless (code injection)
- process doppelganging
- Environmental awareness

*Verizon data breach investigations report 2019
About RaaSberry

RaaSberry provides customized ransomware packages that are ready to distribute. The packages are pre-compiled with a Bitcoin address you provide, and we do not receive any form of payment from your victims.

We also provide a Command and Control (C&C) Center to manage your victims and view individual AES keys.

How does it work?

Once the ransomware is executed on your victim's computer, it will encrypt every file type that was specified when you created it. It examines all local drives and mapped network drives, and encrypts the files with a unique 265-bit AES key that is generated on-the-fly. The AES key is then encrypted using your unique RSA key and uploaded.

Upon completion, the desktop wallpaper will be changed to an image with instructions for paying the ransom. A text file is also created in each folder where there are encrypted files with instructions. The instructions are available in English, Spanish, Mandarin, Hindi, Arabic, Portuguese, Russian, Japanese, German, Italian, Vietnamese, Korean, French, Tamil, and Punjabi.

After the victim has paid, the AES key is provided back to the program to allow decryption. Many ransomware programs require the victim to download a separate decrypter, but RaaSberry has built-in decryption once the C&C server provides the AES key. If you are not subscribed to the C&C service, you can still provide decryption service via email by manually decrypting the victim’s AES key.
Case Studies
Case study #1 – Transportation industry

Day -120
User opens phishing email attachment – Emotet is launched

Day -1
Trickbot is downloaded and launched

D-Day
Ryuk is downloaded and launched

D +10
Trusted network recovery – critical systems back online

D +20
Recovery of all servers

Work Stream 1: Investigation
Determine safe recovery date & find patient zero

Work Stream 2: Recovery
Reconstruct trusted network & deploy backups

>40 locations crippled by the incident
50 people fulltime to keep operations running

2 seconds to compromise the first machine
13 seconds to compromise the first 2000 devices
Case study #1 – Key takeaways

1. Backups, backups, backups
2. Never enough logs
3. The need for dedicated security personnel/role
Case study #2 – Manufacturing industry

Unknown
Patient zero not found because older than log retention

Day -1
Threat Intel source relays potential compromise

Day 0
Compromise assessment confirms compromise

D +1
Containment performed before ransomware detonated

D +10
Collected IoCs allowed complete remediation throughout the environment

Log retention bottleneck
Limited log storage regularly limits the investigation stream

Threat Intel & Threat Hunting
Being aware of threatening actors and being able to proactively search for signs of compromise drastically reduces incident impact

Operational resiliency
A true marker of cyber maturity is being able to maintain operations whilst handling the incident
Case study #2 – Key takeaways

1. Integrated security controls can save your company

2. Hunting IoCs is an integral part of the recovery process

3. Inventory & contextual awareness are half the battle
Lessons from the Field
Lessons from the field

Here are 5 key takeaways from our numerous encounters with ransomware:

- Don’t expose yourself
- You can’t stop what you can’t see
- If you are not prepared, you pay
- Security is a business issue
- Call for help, fast
Questions

Thank you for listening!

Feel free to connect with us

/in/wilfred-farias/
wifarias@deloitte.ca

/in/thomaspc/
tpoinsignonclavel@deloitte.ca