

# Pay Up or Else Critical Knowledge for Ransomware Detonation Response



Jeff Hamm



2022-10-25



DCSO Booth: Hall 6, Nr. 430

# Agenda

## 1

### Ransomware Response

Introduction

IR Readiness

Expanded Teams

## 2

### Lessons Learned

Case Studies

## 3

### To Pay or Not to Pay

What is eCurrency?

When Does the Clock Start Running

What is a Ransomware Negotiator?

Will My Insurance Cover an Investigation?

## 4

### Conclusions

Key Takeaways



# Let's get to know each other



Jeff Hamm

IR Director Cyber Defense Services

- 10 Years Incident Response Consultant
- 20 Years in Digital Forensics
- Assistant professor for cybercrime investigation and digital forensics
- 15 years law enforcement experience as a supervisor, patrolman, and computer crime detective
- Published contributing author "Digital Forensics" (2017 edited by André Årnes)

# Ransomware Response



# Ransomware Response

## Introduction

Ransomware attacks haven't subsided despite efforts to shutdown major operational organizations. Defending against them in case an attack gets through your defenses require preparation – both technical and operationally.

- Are the preventable or can you at least mitigate the impact?
- Do you hire a professional negotiating firm?
- How do you setup cryptocurrency in the event you need to pay the ransom?
- When does the clock start running before the attacker discloses the breach?

Ransomware response has flipped the script on traditional APT investigations.



# Ransomware Response

## Technical Incident Response Readiness

### Network Alert and Logging

- SEIM
- Proxy
- DNS
- DHCP
- East-West Logging
- Isolation

### Endpoint Capabilities

- Alerting
- Inspection
- Isolation
- Live Response
- Forensic Acquisition

### Policies and Procedures

- Playbooks
- Contacts
- Response Examples

### IR Team Proficiencies

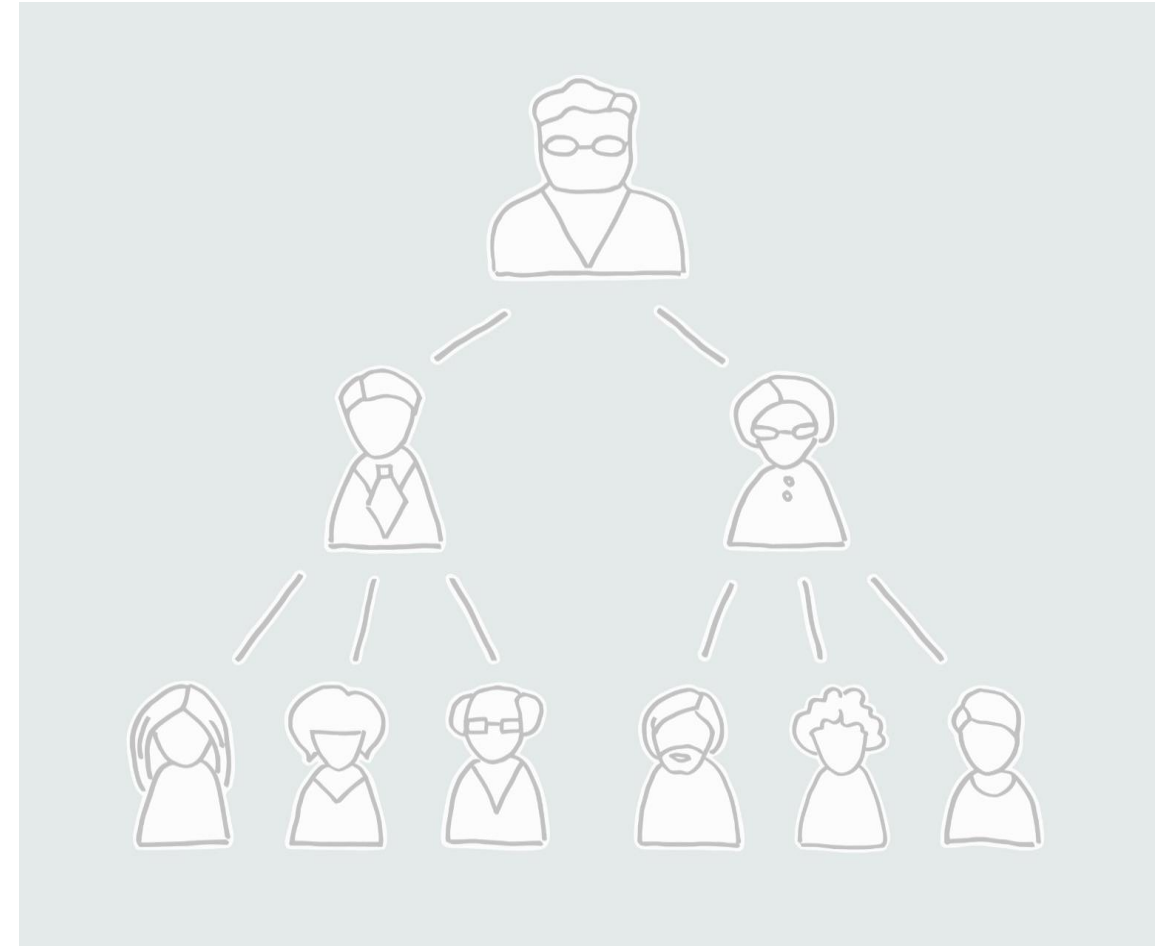
- Ability to Use and Deploy Tools
- Authority Matching Responsibility
- Communication Skills
- Decisiveness



# Ransomware Response

## Expanded Teams Incident Response Readiness

- Disaster Recovery
- Finance
- Human Resources
- Crisis Communications
- Legal Council
- Law Enforcement Contacts
- Executives
- Users/Employees



# Lessons Learned Case Studies



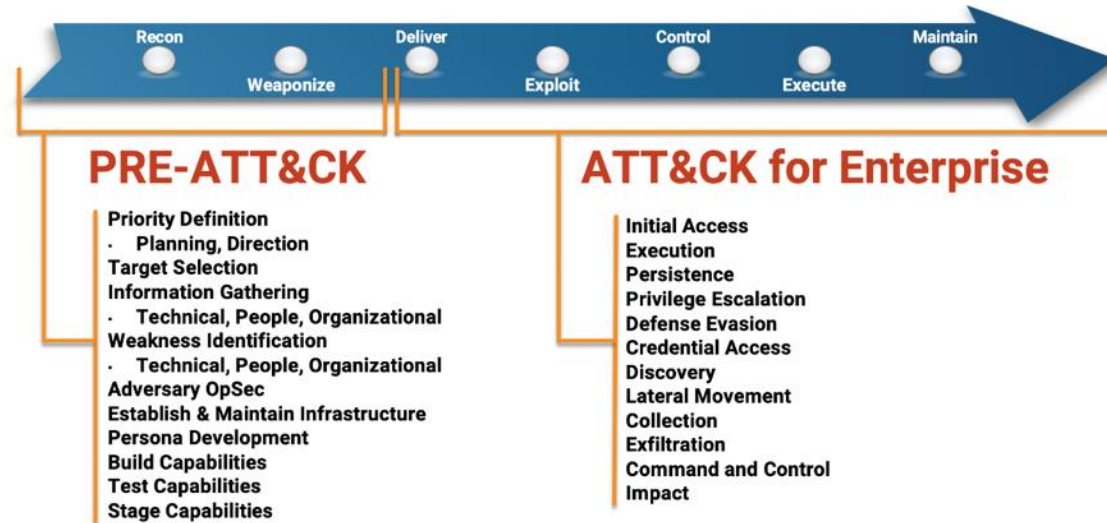


# Lessons Learned

## Disclaimers

### Anonymized Data

The case study data is from actual cases but is anonymized to protect the victim.



### MITRE ATT&CK Framework<sup>1</sup>

A framework that can be used to model attacks and subsequently create better detections and prevention.

# Lessons Learned

## Access Brokers

- **Initial Compromise:**
  - User with admin rights browsed to the Internet from a server
  - “Drive-By” attack
- **Execution:**
  - CobaltStrike “adversary simulation”<sup>2</sup>
- **Persistence:**
  - Attacker gained access to a non-MFA VPN
- **Privilege Escalation:**
  - Admin / System level privileges obtained on initial compromise
- **Defense Evasion:**
  - No disk-based backdoors installed
  - Process injection into legitimate, signed processes
- **Credential Access:**
  - Mimikatz
- **Discovery:**
  - Remote network services from an internal server
- **Lateral Movement:**
  - PSEXEC and RDP
- **Collection:**
  - 7Zip compression from file shares
- **Exfiltration:**
  - Uploads to anonymous internet file servers
- **Command and Control:**
  - Multiple domains registered in a short time frame to one “gmail” address / account

THREAT

# SocGholish

SocGholish leverages drive-by-downloads masquerading as software updates to trick visitors of compromised websites into executing malware.

<https://redcanary.com/threat-detection-report/threats/socgholish/>



# Lessons Learned

## Native Encryption

- **Initial Compromise:**
  - Microsoft Exchange Server
    - ProxyLog Shell
- **Execution:**
  - WebShell
  - RDP tunneling tool
- **Persistence:**
  - Webshell
- **Privilege Escalation:**
  - Vulnerability allowed for System level privileges
- **Defense Evasion:**
  - Waited one year before moving laterally
- **Credential Access:**
  - ProcDump of the LSASS process
- **Discovery:**
  - Webshell functionality
- **Lateral Movement:**
  - RDP through tunneling
- **Collection:**
  - NONE
- **Exfiltration:**
  - NONE
- **Command and Control:**
  - Xhost Cloud Hosting (Netherlands)<sup>3</sup>



Hello. All your servers are encrypted.

Please contact: Ka  
spare email: Ka  
Your identity code

Contact us to get the decryption method. You can first understand how to buy Bitcoin

Only we can decrypt, please do not believe any decryption tool. Your recovery method

## manage-bde

Article • 03/03/2021 • 2 minutes to read • 7 contributors



Turns on or turns off BitLocker, specifies unlock mechanisms, updates recovery methods, and unlocks BitLocker-protected data drives.

### Note

This command-line tool can be used in place of the BitLocker Drive Encryption Control Panel item.

## Syntax

Copy

```
manage-bde [-status] [-on] [-off] [-pause] [-resume] [-lock] [-unlock] [-autour  
[-setidentifier] [-forcerecovery] [-changepassword] [-changePIN] [-changekey] |
```

# Lessons Learned

## Malware-Less Attacks

- **Initial Compromise:**
  - Spear-phishing email posing to sales account manager as an actual account (minor misspelling in the domain) (Emotet)
- **Execution:**
  - CobaltStrike
- **Persistence:**
  - Multiple backdoors on servers
- **Privilege Escalation:**
  - Procdump of the LSASS memory
- **Defense Evasion:**
  - None
- **Credential Access:**
  - ProcDump of the LSASS process
- **Discovery:**
  - Emotet capabilities
- **Lateral Movement:**
  - Emotet
- **Collection:**
  - Possible via RCLONE
- **Exfiltration:**
  - NONE
- **Command and Control:**
  - Emotet generated domains

Subject: "Your data assets were encrypted"

Ok, you are reading this - so it means that we have your attention.

Here's the deal :

1. We breached your internal network and took control over all of your systems.
2. We analyzed and located each piece of more-or-less important files while spending weeks inside.
3. We exfiltrated anything we wanted (the total size of taken data is     GB BUT it is very sensitive and very confidential. Our team attacked you pointwise)

You can find a listing of some taken files in attached file. If you want to see full listing of files you must contact us.

FAQ:

- Who the hell are you?|

- The Karakurt Team. Pretty skilled hackers I guess.

- WHY ARE YOU DOING THIS?!??

- Our motivation is purely financial.

- We are going to report this to law enforcement.

- You surely can, but be ready that they will confiscate most of your IT infrastructure, and even if you later change your mind and decide to pay - they will not let you.

- Who else already knows about the breach?

- Me and You who received the same message the same way. Nobody else. For now.

- What if I tell you that I do not care and I am going to ignore this incident.

- That's a very bad choice. If you will not contact us in a timely manner ( ,     ) we will start notifying your employees, clients, partners, subcontractors and any other persons that should know how you treat your own corporate secrets and theirs.



# To Pay or Not to Pay






## What is eCurrency?



# To Pay or Not to Pay

## What is eCurrency?

“A cryptocurrency is a digital asset that can circulate without the centralized authority of a bank or government. To date, there are more than 20,000 cryptocurrency projects out there that represent the entire \$952 billion crypto market.”<sup>4</sup>

#	Name	Price	1h %	24h %	7d %	Market Cap ⓘ	Volume(24h) ⓘ
☆ 1	 Bitcoin BTC	\$19,535.65	▲ 0.91%	▲ 1.78%	▲ 2.45%	\$374,050,337,916	\$29,720,543,783 1,523,015 BTC
☆ 2	 Ethereum ETH	\$1,325.64	▲ 0.63%	▲ 2.21%	▲ 0.42%	\$162,503,565,554	\$10,497,688,902 7,922,290 ETH
☆ 3	 Tether USDT	\$1.00	▼ 0.00%	▼ 0.00%	▲ 0.00%	\$67,952,114,481	\$39,722,337,424 39,720,764,923 USDT
☆ 4	 USD Coin USDC	\$1.00	▲ 0.02%	▲ 0.01%	▲ 0.02%	\$47,063,330,600	\$4,431,232,778 4,431,049,074 USDC
☆ 5	 BNB BNB	\$288.47	▲ 0.50%	▲ 1.93%	▲ 5.05%	\$46,477,749,453	\$710,936,095 2,467,858 BNB

<https://coinmarketcap.com> October 3, 2022



To Pay or Not to Pay

When does the Clock Start Running?

**As soon as you respond!**



# To Pay or Not to Pay

## What is eCurrency?

- A professional communicator that is experienced in negotiating with criminals
- Ensure everyone is involved in the discussions – law enforcement, legal council, executives
- Some threat actors will not engage with ‘professionals’
- Ensure vetting references
- A risk that the negotiator may be vested in the ransom





# To Pay or Not to Pay

## Will My Insurance Cover an Investigation?

October 3, 2022  
Volume XII, Number 276

THE  
**NATIONAL LAW REVIEW**

October 3, 2022  
Volume XII, Number 276

PUBLISH / ADVERTISE WITH US TRENDING LEGAL NEWS ABOUT US CONTACT US QUICK LINKS ENEWSBULLETINS

1  
NEW ARTICLES

Article By  
Kevin V. Small  
Koorosh Talieh  
Andrea DeField

Hunton Andrews Kurtl  
Hunton Insurance Rec

INSURERS ARE REDUCING OR DROPPING RANSOMWARE  
COVERAGE | MOST COMPANIES LACK A SOLID SECURITY  
PLAN

Posted on March 7, 2022 by Van Oppen Co.

With cyber threats on the rise, now more than ever is the time to implement the best security protocols you can get your hands on. Why? Not only did ransom payouts exceed \$500 Million in 2021, insurers are reducing their coverage amounts, requiring even more risk management and even dropping ransomware coverages altogether.

JOSEPHINE WOLFF SECURITY JUN 12, 2021 7:00 AM

As Ransomware Demands Boom, Insurance Companies Keep Paying Out

While major carriers like AXA have backed away from covering ransoms, don't expect the industry at large to break the vicious cycle.

intelligent  
**CISO**  
security intelligence that  
transcends borders

HOME REGIONS TECHNOLOGY ANALYSIS VIDEOS PODCASTS WHITEPAPER

Search ...

**LATEST NEWS** Research identifies ransomware as top security threat between April-June 2021

How ransomware is destabilising cyber insurance – and what to do about it

BANKING & FINANCE ENTERPRISE SECURITY INSIGHTS INSIGHTS RANSOMWARE THOUGHT LEADERSHIP

TOP STORIES

Alix Pressley | 5 January, 2022



HOME ABOUT US IT SERVICES CLOUD SOLUTIONS IT SECURITY

CYBERSECURITY INSURANCE CARRIERS ARE  
DROPPING COVERAGE & RAISING PRICES



# To Pay or Not to Pay Will My Insurance Cover an I

Yes. But don't expect handcuffs

<https://www.nomoreransom.org/>

Engage with corporate counsel before  
making any decisions

October 3, 2022  
Volume XII, Number 276

## THE NATIONAL LAW REVIEW

PUBLISH / ADVERTISE WITH US TRENDING LEGAL NEWS ABOUT US CONTACT US QUICK LINKS ENEWSBULLETINS

6

NEW ARTICLES

### Russia-Linked REvil Hackers and Their Affiliates Hit with Arrests by the U.S. and International Allies

Tuesday, November 9, 2021

On November 8, 2021, law enforcement agencies in both the United States and European Union announced that a series of actions, including a number of arrests, were taken against the Russian-linked ransomware group, "REvil." The U.S. Department of Justice announced that it had secured documents related to the group's operations.

Article By

Hunton Andrews Kurth's Privacy and  
Cybersecurity

Hunton Andrews Kurth  
Privacy and Information Security Law Blog-  
Hunton Andrews Kurth

LATEST LEGAL NEWS

Neither Snow  
Night . . . Will  
Epstein Becker &

Unpacking A  
Processing t  
Epstein Becker &

ENRPA Fact  
I.D.

### Six Members of the "Cl0p" Ransomware Group Were Arrested in Ukraine

By Bill Toulas / June 17, 2021

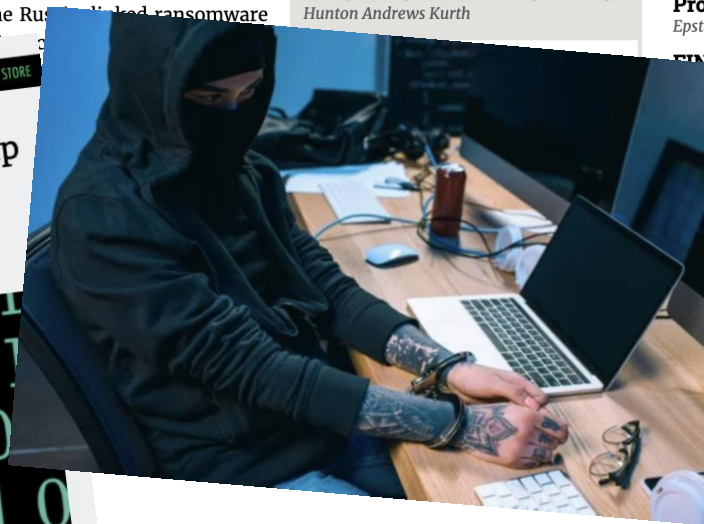


ars TECHNICA

### A week after arrests, Cl0p ransomware group dumps new tranche of stolen data

Leak shows that, like the rest of the ransomware scourge, Cl0p isn't going away.

DAN GOODIN - 6/22/2021, 10:07 PM



TLP: GREEN

WATCH NOW

OPINION

BUSINESS

COVID

WORLD

U.S. NEWS

PLAN YOUR VOTE

POLITICS

HURRICANE IAN

SECURITY

## FBI tracking more than 100 active ransomware groups

While some ransomware gangs have gone silent, many continue to operate, pointing to the challenge authorities face in cracking down on the problem.



# Conclusions

## Key Takeaways





# Conclusions

## Key Takeaways

- Pre-Define a Crisis Communications Team
- Validate Cyber Insurance Contracts
- Integrate with Disaster Recovery Teams
- Plan for Law Enforcement Communications
- Ensure the Finance Team is Familiar with Crypto Currencies
- Effective Response from the Security Team



# References



# Endnotes

1. <https://attack.mitre.org/>
2. <https://www.cobaltstrike.com/>
3. <http://isxhost.com/>
4. <https://www.forbes.com/advisor/investing/cryptocurrency/top-10-cryptocurrencies/>



# Ransomware Articles


## Impacts to Insurance Providers

- <https://www.natlawreview.com/article/ransomware-2022-you-may-be-screwed-without-insurance-it-could-always-be-worse>
- <https://www.wired.com/story/ransomware-insurance-payments/>
- <https://www.vanoppenco2.com/insurers-are-reducing-or-dropping-ransomware-coverage-most-companies-lack-a-solid-security-plan/>
- <https://www.haxxess.com/cybersecurity-insurance-raising-prices>
- <https://www.intelligentciso.com/2022/01/05/how-ransomware-is-destabilising-cyber-insurance-and-what-to-do-about-it/>

## Law Enforcement Efforts

- <https://edition.cnn.com/2021/10/04/politics/ransomware-arrests-ukraine/index.html>
- <https://www.nbcnews.com/tech/security/fbi-tracking-100-active-ransomware-groups-rcna1524>
- <https://www.technadu.com/six-members-clop-ransomware-group-arrested-ukraine/284275/>
- <https://arstechnica.com/gadgets/2021/06/a-week-after-arrests-cl0p-ransomware-group-dumps-new-tranche-of-stolen-data/>





**Let's meet!**  
Hall 6, Booth 430

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH  
EUREF-Campus 22  
10829 Berlin

[jeff.hamm@dcso.de](mailto:jeff.hamm@dcso.de)

+49 151 72140869