Ransomware in Healthcare

Financial Fallout, Operational Risk, and Third-Party Exposure

Introduction

Michael Rieger

Security Operations Manager - BCI

Why This Matters Now?

- Healthcare remains a top target for ransomware
- Attackers perceive a high willingness to pay due to patient impact.
- Increasing dependence on interconnected systems

A Real-World Wake-Up Call

- Change Healthcare Attack
- Group was ALPHV/BlackCat
- Widespread Impact

Medusa

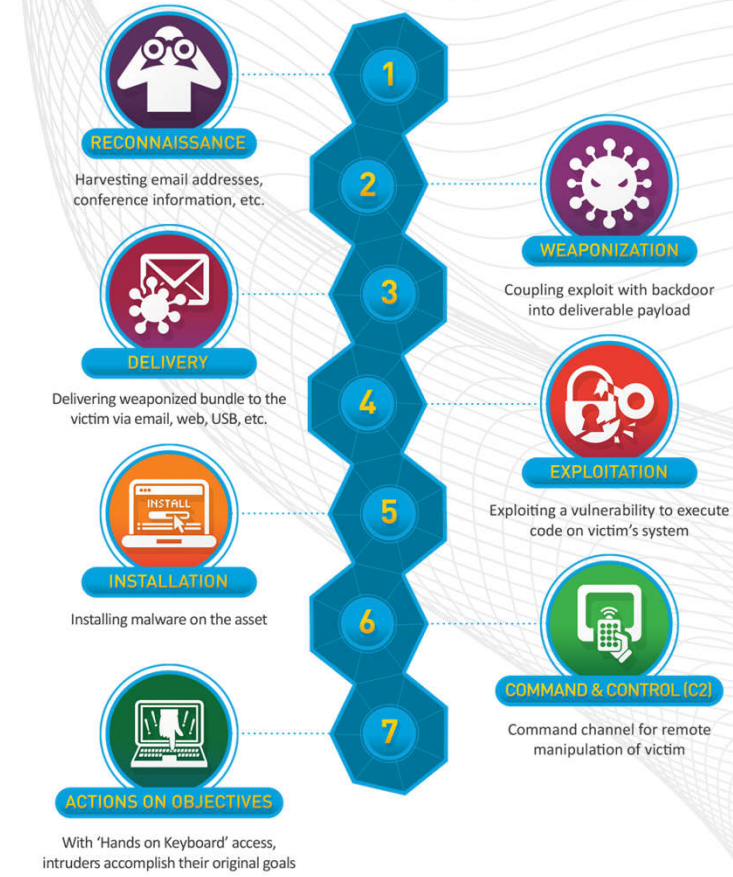
Qilin

INC Ransomware

RansomHub

The Modern Ransomware Business Model

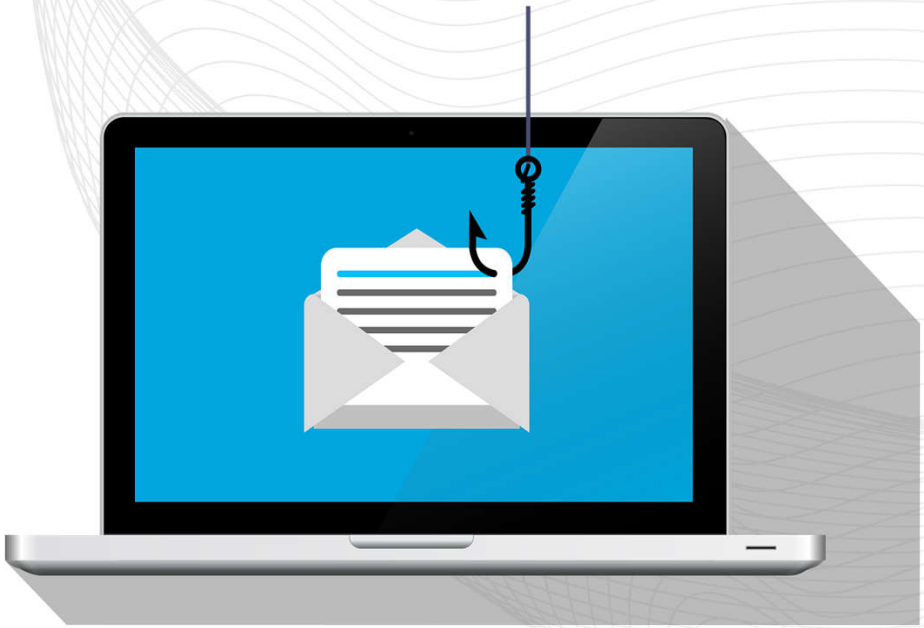
- Not always just encryption
- Double/Triple Extortion
- Professionalization of Cybercrime
- Large Ecosystem



https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

How Attacks Actually Start

- Phishing is still widely used
- Credential theft and fatigue attacks
- Third-party/vendor access has grown

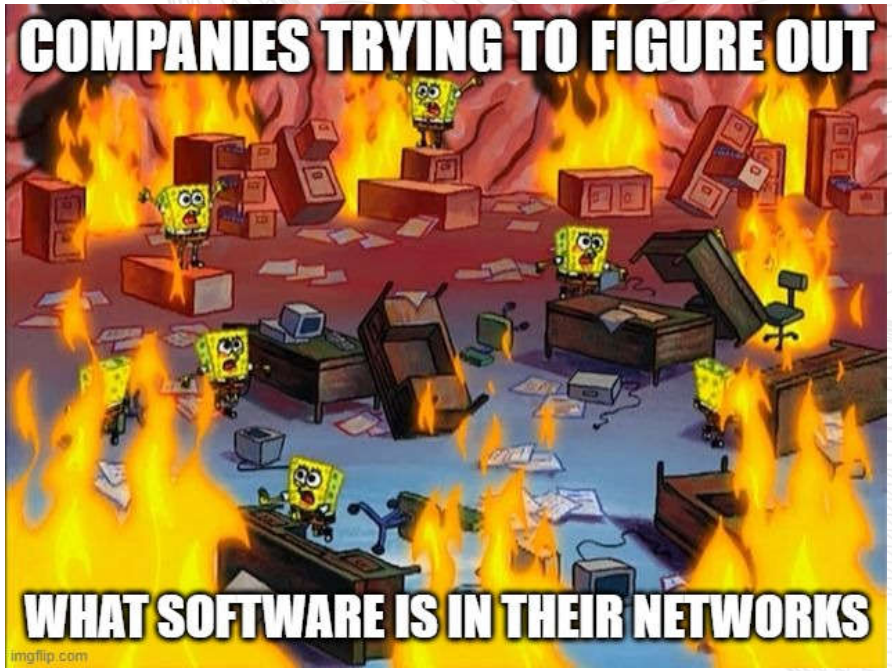


Third Parties Can be a Weak Link

- Vendors may lack mature security programs
- Too much trust in compliance
- Limited visibility into vendor environments
- Keeping up with patching and vulnerability releases

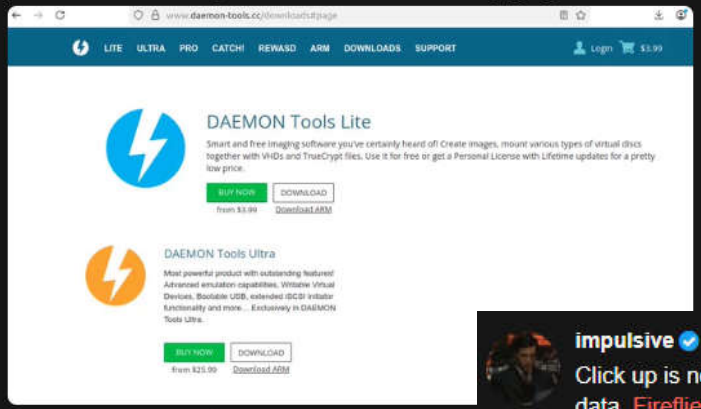
Supply Chain attacks

- These remain something to keep an eye on
- Can be opportunistic but occasionally targeted



Georgy Kucherin @kucher1n 4h

Together with @bzvr_, @2igosha and Anton Kargin, we identified that the DAEMON Tools software has been compromised in a complex supply chain attack since April 8. We see thousands of infections across 100+ countries. If you use DAEMON Tools, run a malware scan immediately! [1/7]

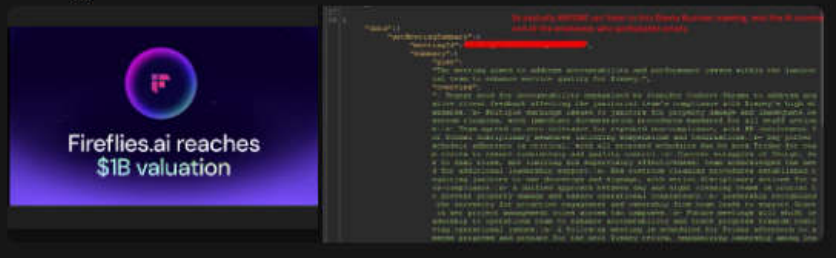


7 139 376 34,728

impulsive @weezerOSINT Apr 27

Click up is not the only multibillion dollar funded AI company exposing your data. Fireflies.ai allows anyone with an unauthenticated request download the FULL Call audio and video + including emails to every participant and an AI summary of your private meeting.

Below is a Disney meeting Call summary and how they're deciding to improve or fire the janitors who leave dirty toilets. That's just a small segment of the meeting.



TreyCraf7 @TCraf7 Apr 27

Six months..
That's how long Lotus Blossom owned Notepad++'s update infrastructure while delivering the Chrysalis backdoor to selected targets.

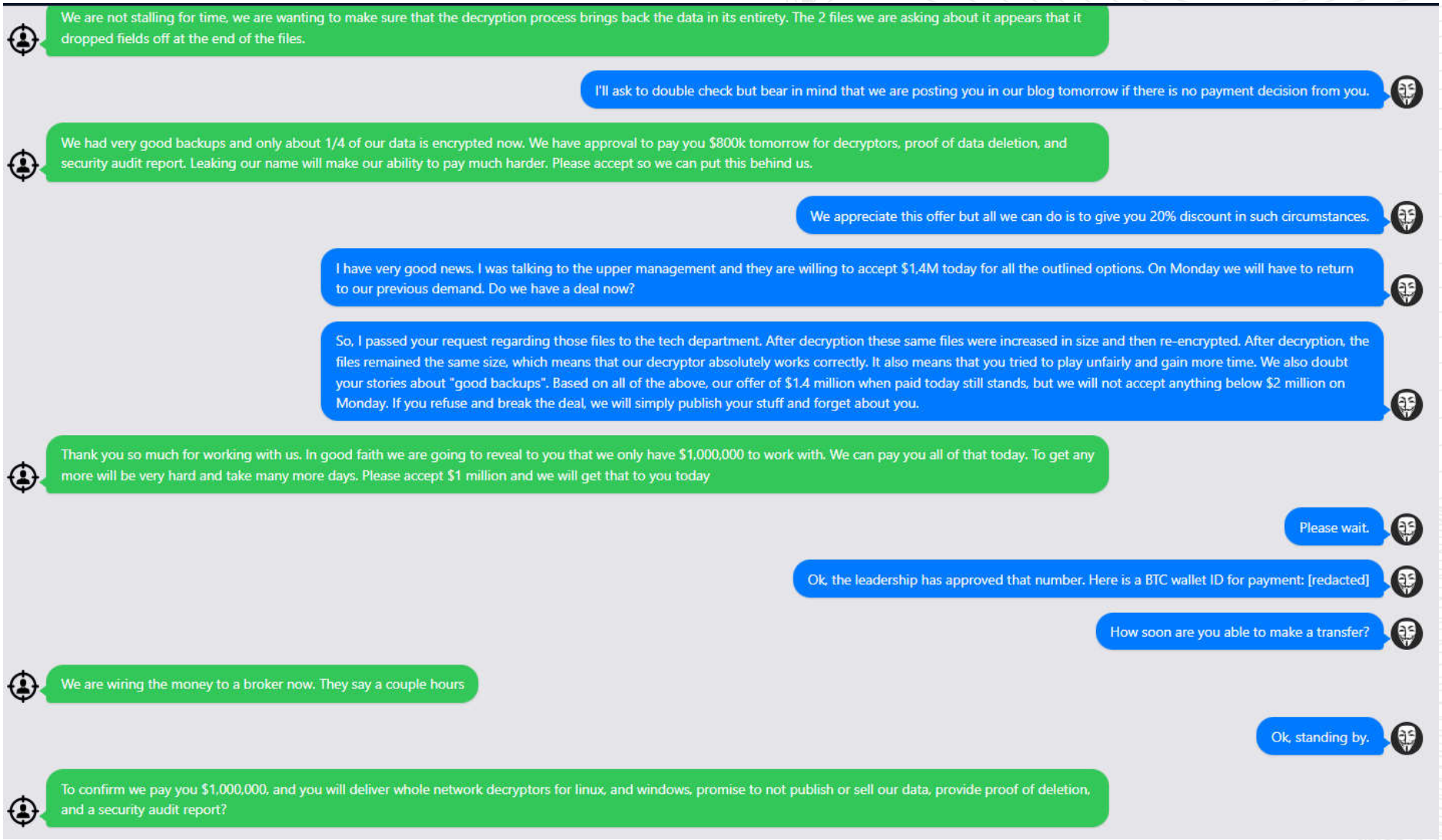
Supply chain attacks don't bypass your detection. They bypass your suspicion.

I wrote a quick breakdown of their campaign found here:
scythe.io/scythe-labs/notepa...
(1/2)
#SupplyChainSecurity #ThreatIntel #DetectionEngineering

1 8 38 3,629

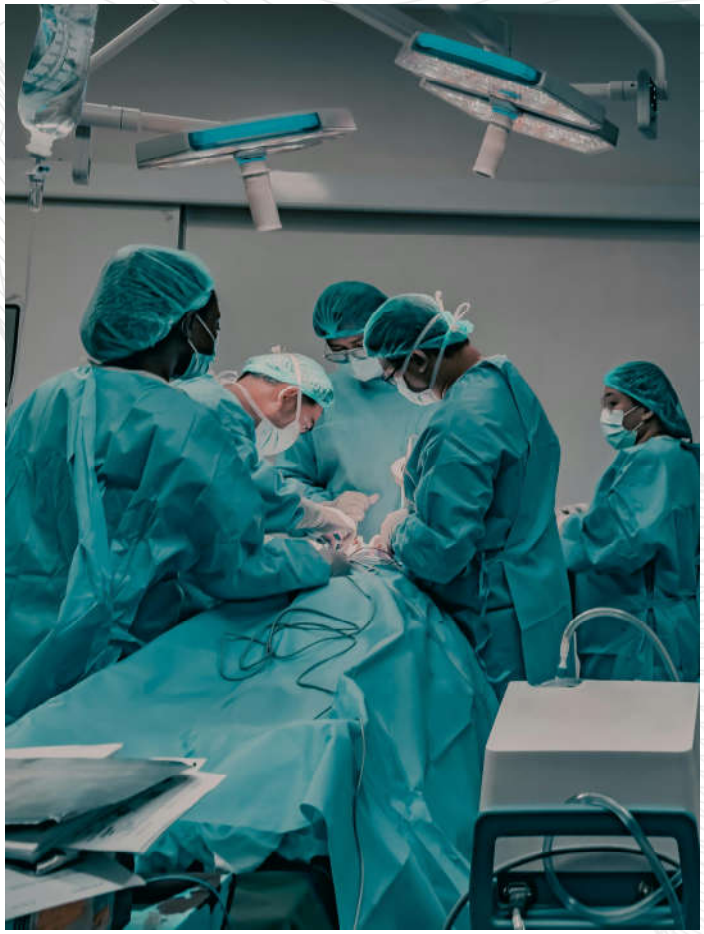
Financial Impact: Direct Costs

- Ransom payments (potential)
- Incident response and forensics
- Legal and regulatory costs
- System restoration


We are not stalling for time, we are wanting to make sure that the decryption process brings back the data in its entirety. The 2 files we are asking about it appears that it dropped fields off at the end of the files.
I'll ask to double check but bear in mind that we are posting you in our blog tomorrow if there is no payment decision from you.
We had very good backups and only about 1/4 of our data is encrypted now. We have approval to pay you $800k tomorrow for decryptors, proof of data deletion, and security audit report. Leaking our name will make our ability to pay much harder. Please accept so we can put this behind us.
We appreciate this offer but all we can do is to give you 20% discount in such circumstances.
I have very good news. I was talking to the upper management and they are willing to accept $1,4M today for all the outlined options. On Monday we will have to return to our previous demand. Do we have a deal now?
So, I passed your request regarding those files to the tech department. After decryption these same files were increased in size and then re-encrypted. After decryption, the files remained the same size, which means that our decryptor absolutely works correctly. It also means that you tried to play unfairly and gain more time. We also doubt your stories about "good backups". Based on all of the above, our offer of $1.4 million when paid today still stands, but we will not accept anything below $2 million on Monday. If you refuse and break the deal, we will simply publish your stuff and forget about you.
Thank you so much for working with us. In good faith we are going to reveal to you that we only have $1,000,000 to work with. We can pay you all of that today. To get any more will be very hard and take many more days. Please accept $1 million and we will get that to you today
Please wait.
Ok, the leadership has approved that number. Here is a BTC wallet ID for payment: [redacted]
How soon are you able to make a transfer?
We are wiring the money to a broker now. They say a couple hours
Ok, standing by.
To confirm we pay you $1,000,000, and you will deliver whole network decryptors for linux, and windows, promise to not publish or sell our data, provide proof of deletion, and a security audit report?

Financial Impact: Indirect Costs

- Lost revenue from downtime
- Delayed billing and claims
- Patient diversion
- Reputational damage



Operational and Cashflow Impacts

- Claims processing interruptions hit liquidity fast
- Downtime Affects care delivery
- Canceled procedures
- Staff productivity decrease

Patient Safety

- Delayed Diagnostics and treatment
- Manual processes could increase error rates
- Essentially, cybersecurity can become a patient safety issue
- Harm from potential leak of PHI

Where do Organizations go wrong

- Overreliance on perimeter defenses
- Poor identity access controls
- Lack of tested incident response plans
- Blind trust in vendors

Cyber Insurance

- Understand your coverage
- Claim denials
- Rising costs
- Insurance shouldn’t be the only strategy

What Can Be Done?

- Inventory of critical vendors
- Risk tiering
- Continuous monitoring
- Planning and testing
- Network Edge Security
- Update and Patch
- Back Ups

Resilience and Prevention

- You may not be able to stop everything
- How to minimize downtime?
- Recovery speed

Planning

- Downtime tolerance (hours, days?)
- Actual recovery time vs business expectations
- Vendor dependencies
- Incidence cost per day

Investment Tradeoffs

- Prevention vs detection vs response
- Security vs resilience spending
- Look to spend smartly

Summary

- Ransomware is a business risk, not just an IT problem
- Third-party exposure can be a major risk
- Prioritize resilience and prevention

Questions?