

2025 Ransomware Realities: How AI is Changing the Game, and What Businesses Must Do

Dennis Underwood
CEO, Cyber Crucible, Inc.

Did some cool cyber stuff that got the government's
attention.

"Most likely to create demo videos that receive malicious
DMCA takedowns"



Gratuitous LinkedIn QR code.



1

Ransomware is a Business Problem - 2019 vintage

Only 3 minutes difference

The same key

RSA1 binary data

2



Why Extortion & Blackmail? Because of the onions.

Onion Futures Act - 1950's



"The Bad Guy"



3

Workforce Challenges for the Busy Extortion Executive

1. Generating leads (AKA, gaining access to more potential victims)
2. Executing sales operations (AKA, running double extortion operations)
3. Supporting delivery and payment from customer (AKA, decryption and ransom payment)

"The Bad Guy"



"The Henchmen"



4

(Extortion) Supply Chain Issues for the Executive

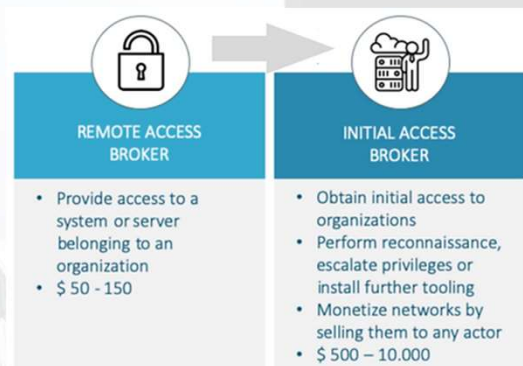
- I need more leads = I need access to more victim companies.
- I need more partners to process leads = I need access to extortion resellers.
- I have too many sales to process = I need a support center to handle the ransom payment calls.
- I'm losing sales to competitors = I need to optimize my product to reliably beat security tools and teams.

"I want to grow my revenues faster, with more predictability in my sales. How do I enable my teams to work as efficiently as I do in all stages of sales pipeline? How do I multiply my efforts?"
 –The Bad Guy, probably



5

Outsourcing Provides Some Sales Operations Support



"Ransomware as a Service"



6

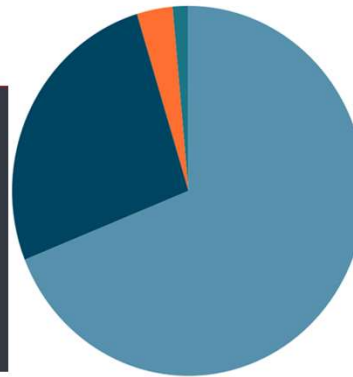
Identity drives data → Robotic Process Automation edition

- “Identity” data
- How attackers normally operate

Identity Theft Target Application

Category	Count
Logins	20237
Logins Starter	1275811
Builder	124028
Notifications	22
Settings	23
Contacts	33

Top 10 of OS	
Windows 10 Enterprise x64	423
Windows 10 Home x64	184
Windows 7 Ultimate x64	119
Windows 10 Pro x64	71
Windows 7 Professional x64	61
Windows 8.1 Pro x64	43
Windows 8.1 x64	12
Windows 8.1 Single Language x64	11
Windows 10 Enterprise x86 1758 x64	11
Windows 7 Home Premium x64	10



7

Customer Acquisition Costs Improving Rapidly

Old Lead Generation

- Static sales call scripts
- Lack of personalization to the “buyer” persona
- Native language issues
- HR for criminal syndicates

Modern Lead Generation

- Hyper-targeting of leads
- Co-opting & impersonation of trusted sources
- Interactive multi-branch conversation trees
- Language issues removed



8

Frictionless Sales Operations & Onboarding



Automate. Automate. Automate.

1. Create programs that automatically perform routine tasks.
2. Distribute programs to Resellers & Employees.
 - a. (Do you as extortionist executive trust these folks anyway?)
3. Update and expand for additional customer environments and "sales objections".



Machine Learning + Robotic Process Automation



9

Personalized Service Wins Deals Over The Competition



Malware

Malware with
Machine Learning
& Robotic Process
Automation



10

Ransomware Statistics -

lies more lies and ransomware statistics

cybercrucible

Lies, More Lies, and Ransomware Statistics

Dennis Underwood
CEO, Cyber Crucible, Inc.

Questionable QR Code

0:11 / 42:38 · Intro >

Lies, More Lies, and Ransomware Statistics - Dennis Underwood

SecPgh
454 subscribers

Subscribe

3

Share

Clip

All Watched

cybercrucible

11

A Dennis Prediction - Payments Personalization Coming True: AKA, Money Laundering 101

Field Effect
<https://fieldeffect.com/blog/ransom-payments-decline...>

Ransom payments decline 35% in 2024, attack frequency ...

Feb 7, 2025 — Ransomware victims paid a total of \$813.5 million. This is down \$436.5 million from 2023, making 2024 the first year since 2022 that ransomware revenues ...

CyberScoop
<https://cyberscoop.com/ransomware-payments-drop-3...>

Ransomware payments dropped 35% in 2024

Feb 5, 2025 — Ransomware payments saw a dramatic 35% drop last year compared to 2023, even as the overall frequency of ransomware attacks increased.

cybercrucible

12