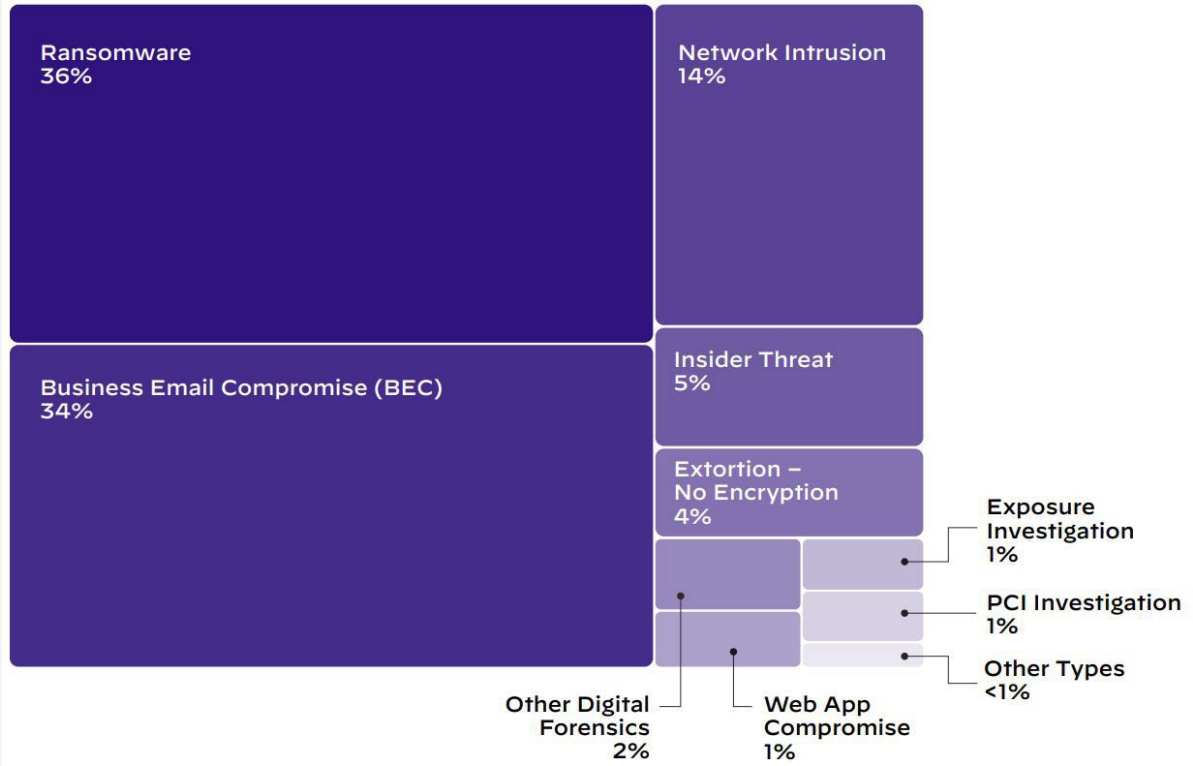
Tales from the Trenches; the Current Cyber Threat Landscape

John Wood
Director, Unit 42


Mark LaVigne, PhD
Deputy Director
NYSAC

What Attackers Are Going After In 2022



Unit 42: The Attacker's Toolkit - Cobalt Strike

WHAT IS COBALT STRIKE

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

- Commercial Adversary Simulation / Red Team Ops
- Emulate post-exploitation actions
- Easy-to-use interface with built-in exploitation and attack packages
- Cover full range of ATT&CK tactics

ATTACKER USES

- First-stage exploitation, second-stage payload
- Establish command and control (C2), remote access
- Reconnaissance activity and lateral movement
- Post-exploitation actions (malware, scripts, keylogging, screenshots, etc.)

INITIAL ACCESS TO ENVIRONMENT
EMAIL | EXPLOIT | CREDS

1

COBALT STRIKE EXECUTED ON COMPROMISED SYSTEM

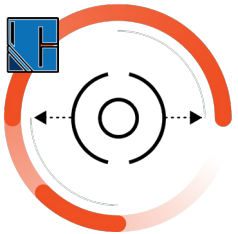
2

C2 ESTABLISHED TO ATTACKER INFRASTRUCTURE

3

RECONNAISSANCE/ CREDENTIAL THEFT ACTIVITY
USERS | SYSTEMS | NETWORK

4



LATERAL MOVEMENT AND STAGING

5

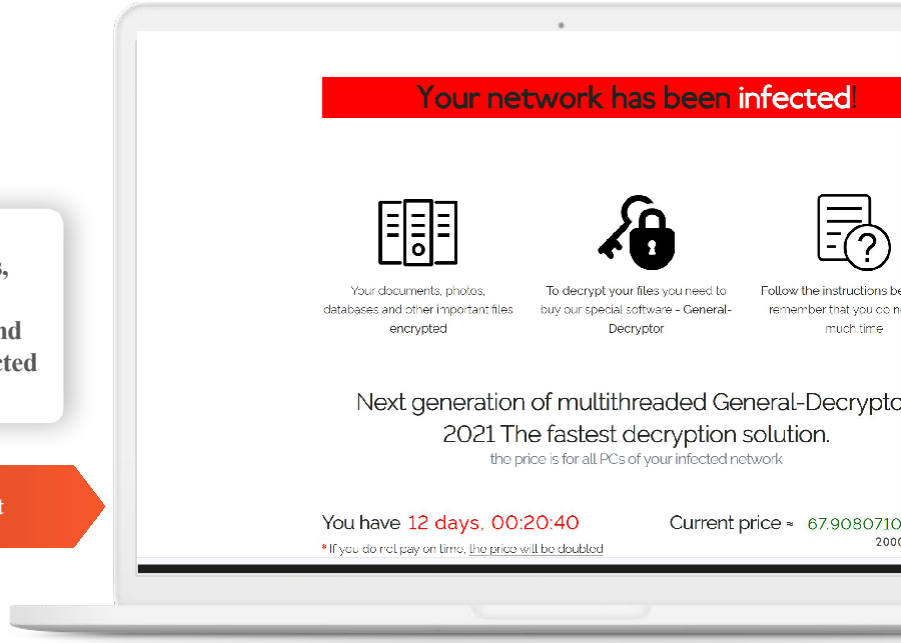
EXECUTION ON OBJECTIVES
RANSOMWARE | DATA THEFT | ESPIONAGE

6

Multi-extortion Techniques

Pressure Organizations To Pay More Quickly

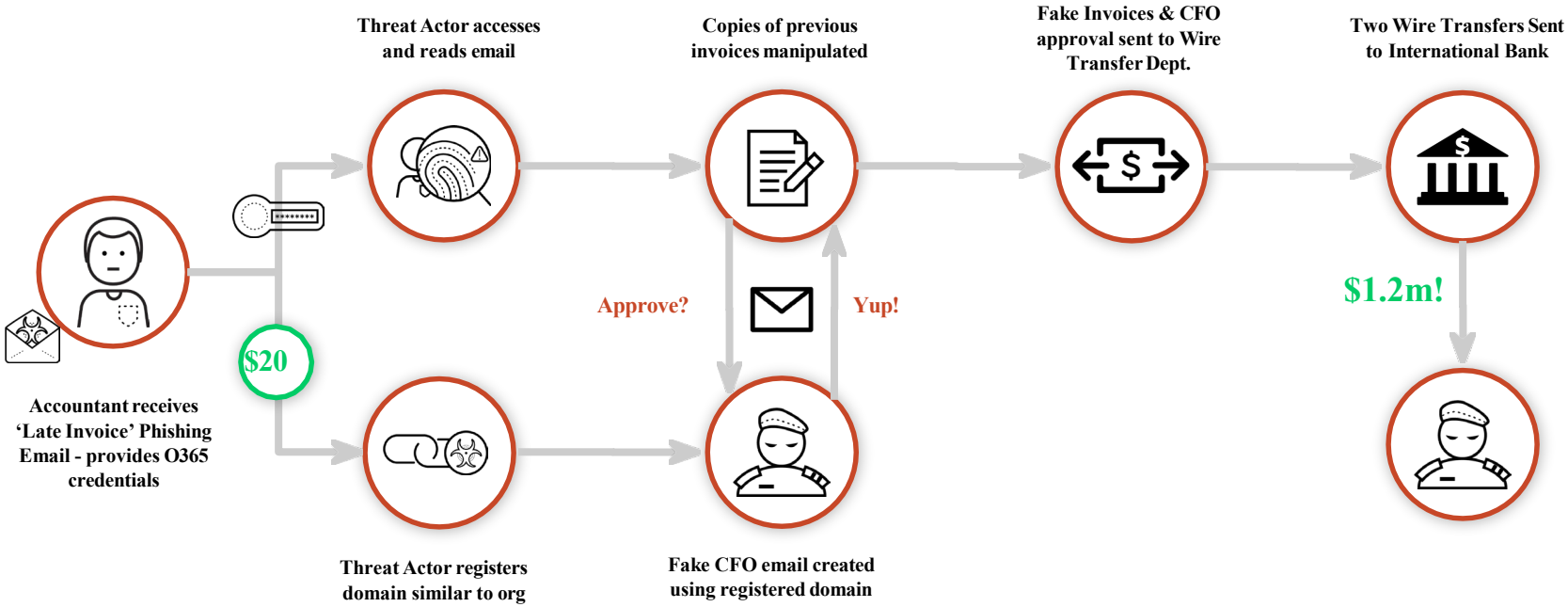
Victims pay to regain access	Hackers threaten to release Stolen data	DoS attacks shut down public websites	Customers, business partners, and media contacted
Encryption	Data Theft	DOS	Harassment



Ransomware Onion Leak Site

Business Email Compromise

How a $20 investment and 7 days of work can earn you $1.2m!



Unit 42

Threat and Ransom Groups

Lazarus Group

Lazarus is a state-backed threat actor

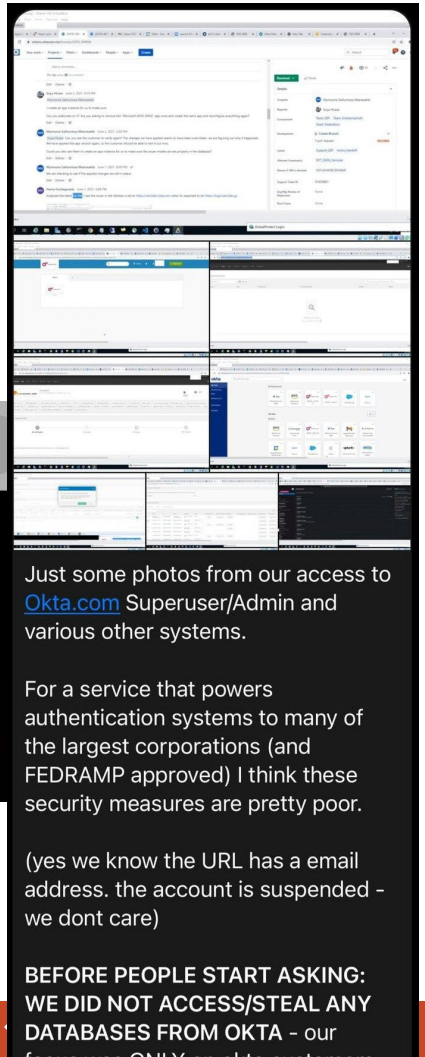
- State-sponsored cyber financially motivated theft
- Tracked as BeagleBoyZ, APT38, Lazarus Group, and Stardust Chollima
- Multiple attributions to North Korea
- Regular targets are Global financial institutions, Foreign Governments
- **Lazarus targeted the energy organizations between February and July 2022[1]**
    - **Leveraging public VMWare Horizon exploits for initial access**

1. Reported by Cisco Talos
2. Lazarus logo from https://apt.securelist.com/apt/lazarus

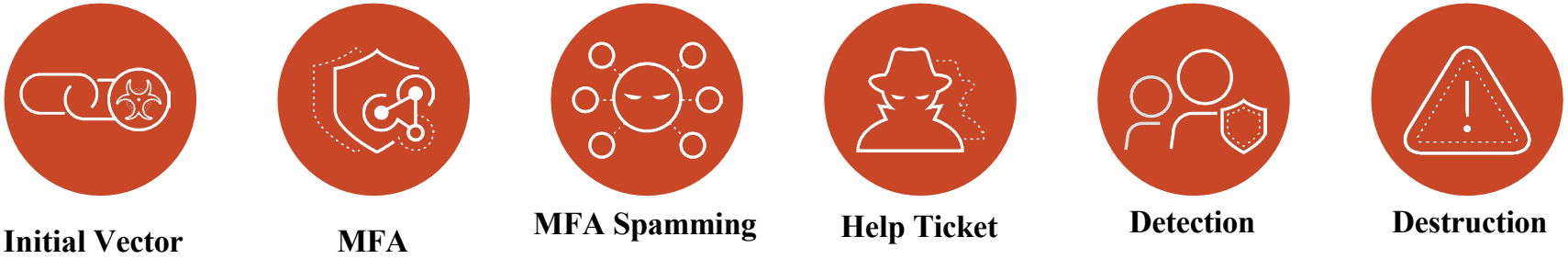
Lapsus$

Lapsus$ - destructive attacks of multiple top-tier technology companies.

- Destructive attacks to stealing and publishing source code of multiple top-tier technology companies.
- Lapsus$ Group doesn't employ malware in breached victim environments, doesn't encrypt data and in most cases, doesn't actually employ extortion.



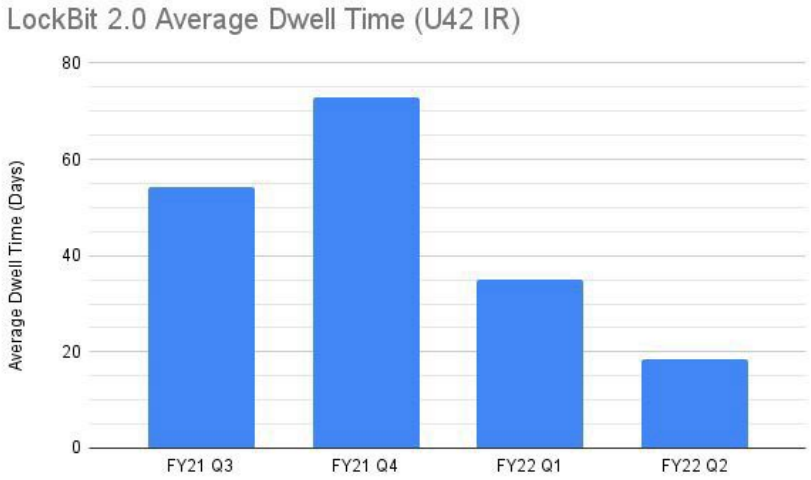
Anatomy of a Lapsus$ Attack



LockBit 2.0 ~~3.0~~ Ransomware

LockBit 3.0

- Avoids systems that use Eastern European languages, including many written with Cyrillic alphabets.
- As of May 25, LockBit 2.0 accounted for 46% of all ransomware-related breach events for 2022.
- LockBit 2.0 RaaS leak site has the most significant number of published victims, with over 850 in total.
- Significant reduction in dwell time before encryption
- New version June 2022 Lockbit 3.0
- Linked to sanctioned entity EvilCorp

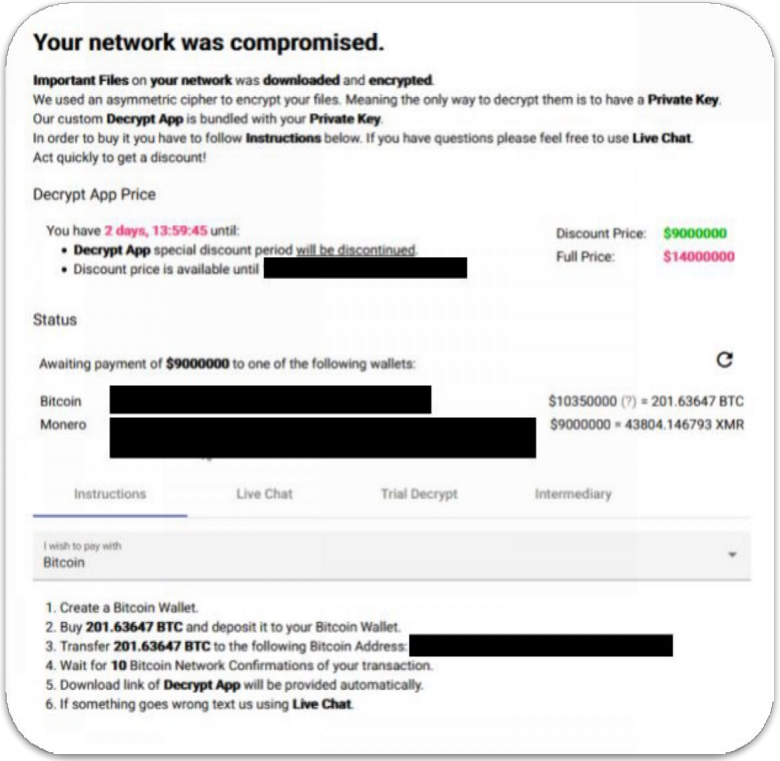


https://unit42.paloaltonetworks.com/lockbit-2-ransomware/

BlackCat/ALPHV Ransomware Group

BlackCat (aka ALPHV) is notable because of the group's meteoric rise

- New group emerged Mid-November 2021
- Offering 80-90% of ransom payment to affiliates, paying 10-20% to ransomware author
- More than a dozen victims in their first month; seventh largest number of victims in just a few months
- Ransomware coded in Rust, enabling for easy cross platform attacks against Windows and Linux.
- Deploying Triple Extortion in some cases (Exfiltrate, Encrypt, DDoS)



Unit 42

Threat actor negotiations

Typical ransomware negotiation process

01	Establish contact, determine threat actor identity, and identify initial terms	• Are they responsive? Who do they identify as? • What is the ransom demand? • Have they given any deadline? • What have they threatened to do if we don't meet it?
02	Verify claims and determine potentially acquired data	• Ask for file listing • Get proof they have these files
03	Verify "proof of life"	• Identify files (not claimed to have been taken) for proof of decryption • Send files to threat actor and verify decrypted files
04	Negotiate the ransom and terms	• Is the threat actor a sanctioned entity? • Whether you are stalling or actually intend to pay, propose an initial offer and stall while you recover and investigate
05	Pay and/or break contact	• Work with payment vendor to pay agreed amount, if applicable • Analyze decryptor for malicious functionality and test for desired functionality and performance • Obtain proof of destruction of acquired data • Obtain promise not to leak / disclose • Cease communications and verify no disclosure on leak site

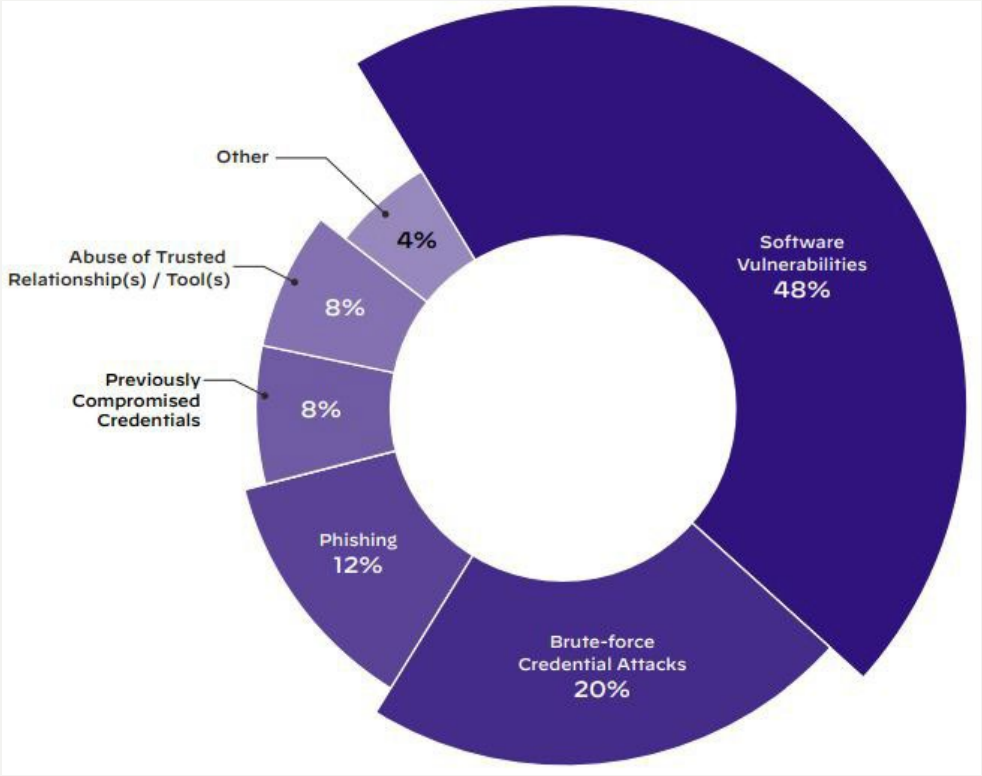
Unit 42

Attack Surface

Perspective

Ransomware: Initial Access

- Attackers are opportunistic and use exposed Software vulnerabilities
- Exposed services without MFA (Such as RDP) allow for Brute force attacks.
- Phishing is still a top vector for access.



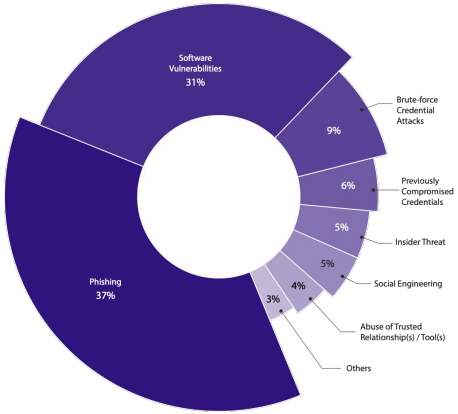
Trend

Increasing Use of Zero Day Attacks

- In 2021, we observed at least **42 vulnerabilities** across different technologies being used by ransomware operators.
- While there is some reliance on older, unpatched vulnerabilities, we believe threat actors are increasingly tracking high-profile vulnerabilities and exploiting them to gain an initial foothold in an organization.
- Unit 42 observed ransomware attacks associated with Microsoft Exchange Server, ProxyShell, Kaseya, Log4j, and other major vulnerabilities.

7 Key Insights

Seven Issues Threat Actors Don't Want You to Address



70%

Phishing and Software Vulnerabilities cause majority of Cyber Incidents

1 Multifactor Authentication

In **50% of cases,** organizations lacked multifactor authentication.

2 EDR / XDR

In **44% of cases**, there was no EDR / XDR solution or it was not fully deployed.

3 Patch Management

In **28% of cases,** poor patch management contributed to threat actor success.

4 Brute-Force Mitigation

In **13% of cases**, no brute force mitigation was in place.

5 Security Alerts

In **11% of cases**, organization failed to review or action security alerts.

6 Password Security

In **7% of cases**, weak passwords contributed to the incident.

7 Misconfigurations

In **7% of cases**, system misconfigurations were a factor.


ASSESSMENT
RANSOMWARE
VULNERABLE
THREAT
ATTACK
CRYPTOJACKING
EXPLOIT
BRIEF
NETWORK
MALWARE
CVE
USE
CLOUD
UNIT
NEW
SERVER
MICROSOFT
TRAFFIC
REPORT
TREND
FILE
AWS
GANG
TOOL
DNS
LEAK
RCE
EXCHANGE
TUTORIAL
GROUP
VARIANT
IOT
RDP
WINDOWS
MALICIOUS
EMOTET
SPREAD
DETECT
FINDING
BLACK
APPLE

Thank You