Trend Micro

Leveraging AI-based XDR in the new threat landscape

Alexandros Vasilakis

Regional Sales Manager – Greece, Cyprus & Malta

Trend Micro At a Glance

$2 Billion 2022 Net Sales

96 Consecutive Profitable Quarters

Every quarter since going public

424,000+ SaaS Commercial Customers

500,000+ commercial customers, 175+ countries

62M+

SaaS-Protected Assets

#1 Cloud Security

Based on global market share*

Leader in **XDR**

Based on offering strength and strategy*

Leader in **EPP**

Based on offering strength and strategy*

#1 Next-Gen IPS

Based on global market share*

#1 in Public Vulnerability Disclosure*

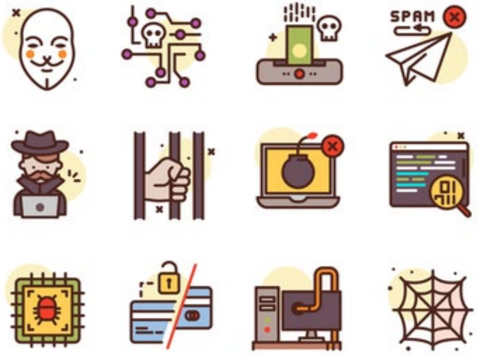
+ Over 140 Billion threats blocked in 2022

7500+ Employees in **73 Countries**

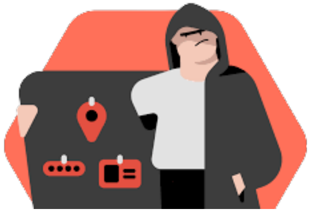
*IDC Worldwide Cloud Workload Security 2021 Share Snapshot, July 2022
*Forrester Wave, Extended Detection and Response (XDR), Q4, 2021
*Gartner Magic Quadrant for Endpoint Protection Platforms, May 2021
*Gartner Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 3Q22
*Quantifying the Public Vulnerability Market, Omdia, May 2022

Threat Landscape

Initial Access

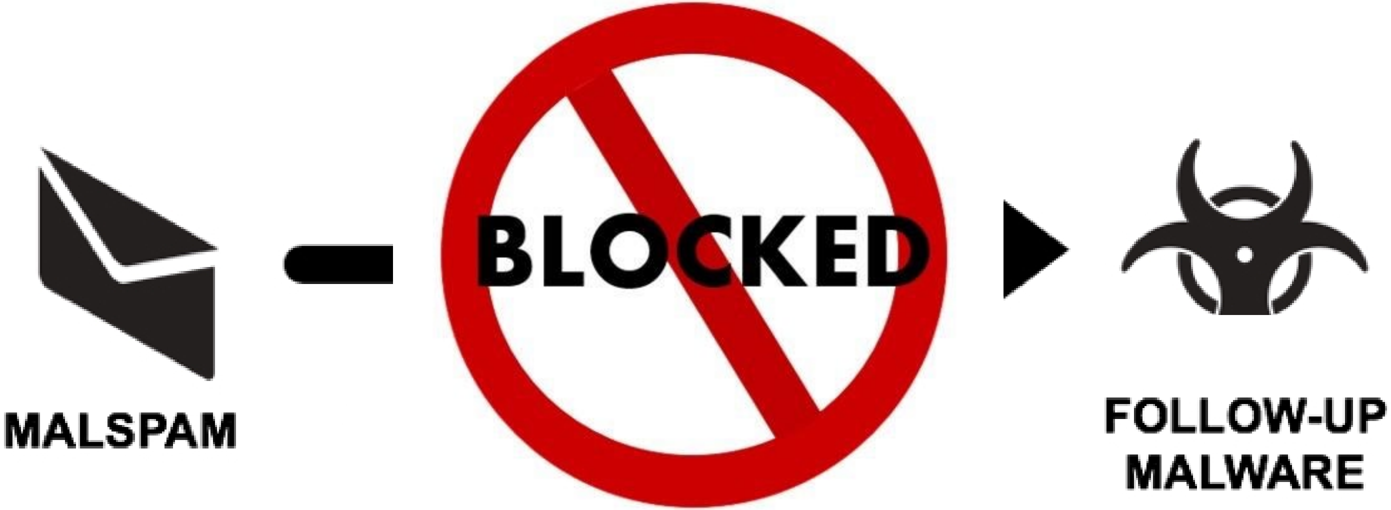


Tools of the Trade

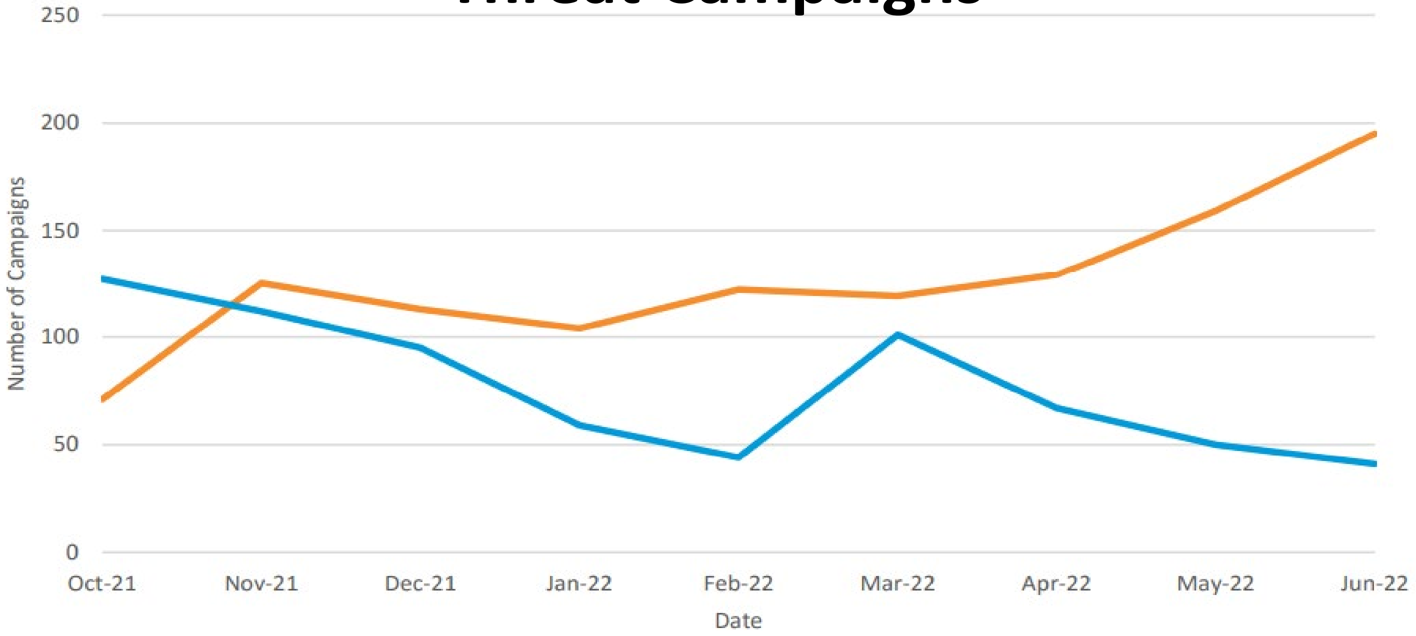


(Financial) Gain

The most popular Initial Access vector.



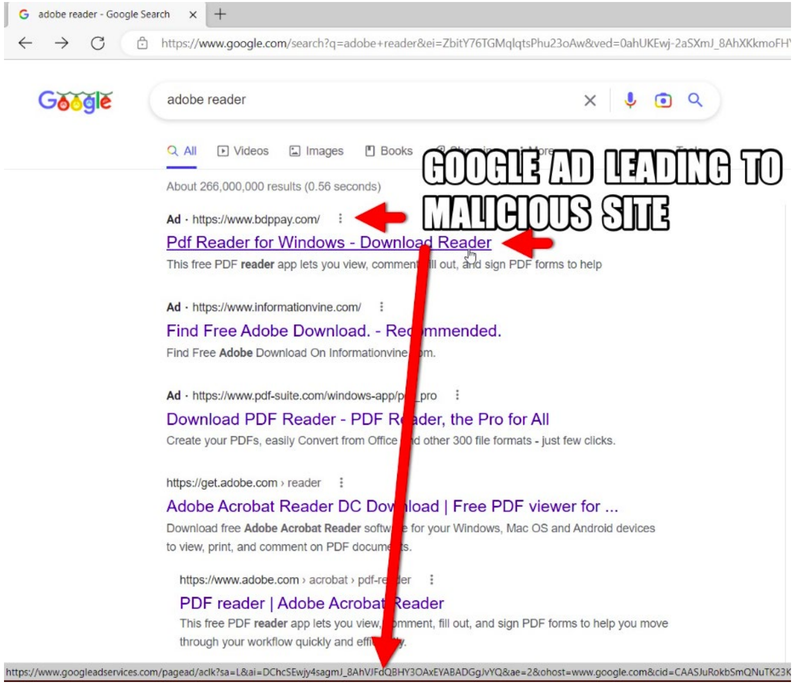
Threat Campaigns



● Using Office Macros

● Using alternative Initial Access vectors

Alternative Initial Access vector … (1)


adobe reader - Google Search
Google
All
Videos
Images
Books
GOOGLE AD LEADING TO MALICIOUS SITE

https://www.google.com/search?q=adobe+reader&ei=ZbitY76TGMqlqtsPhu23oAw&ved=0ahUKEwj-2aSXmJ_8AhXKkmoFH

adobe reader

About 266,000,000 results (0.56 seconds)

Ad · https://www.bdppay.com/

Pdf Reader for Windows - Download Reader

This free PDF **reader** app lets you view, comment ill out, and sign PDF forms to help

Ad · https://www.informationvine.com/

Find Free Adobe Download. - Rec mmended.

Find Free **Adobe** Download On Informationvine om.

Ad · https://www.pdf-suite.com/windows-app/p _pro

Download PDF Reader - PDF R ader, the Pro for All

Create your PDFs, easily Convert from Office d other 300 file formats - just few clicks.

https://get.adobe.com › reader

Adobe Acrobat Reader DC Dow load | Free PDF viewer for ...

Download free **Adobe Acrobat Reader** softw e for your Windows, Mac OS and Android devices to view, print, and comment on PDF docume ts.

https://www.adobe.com › acrobat › pdf-re der

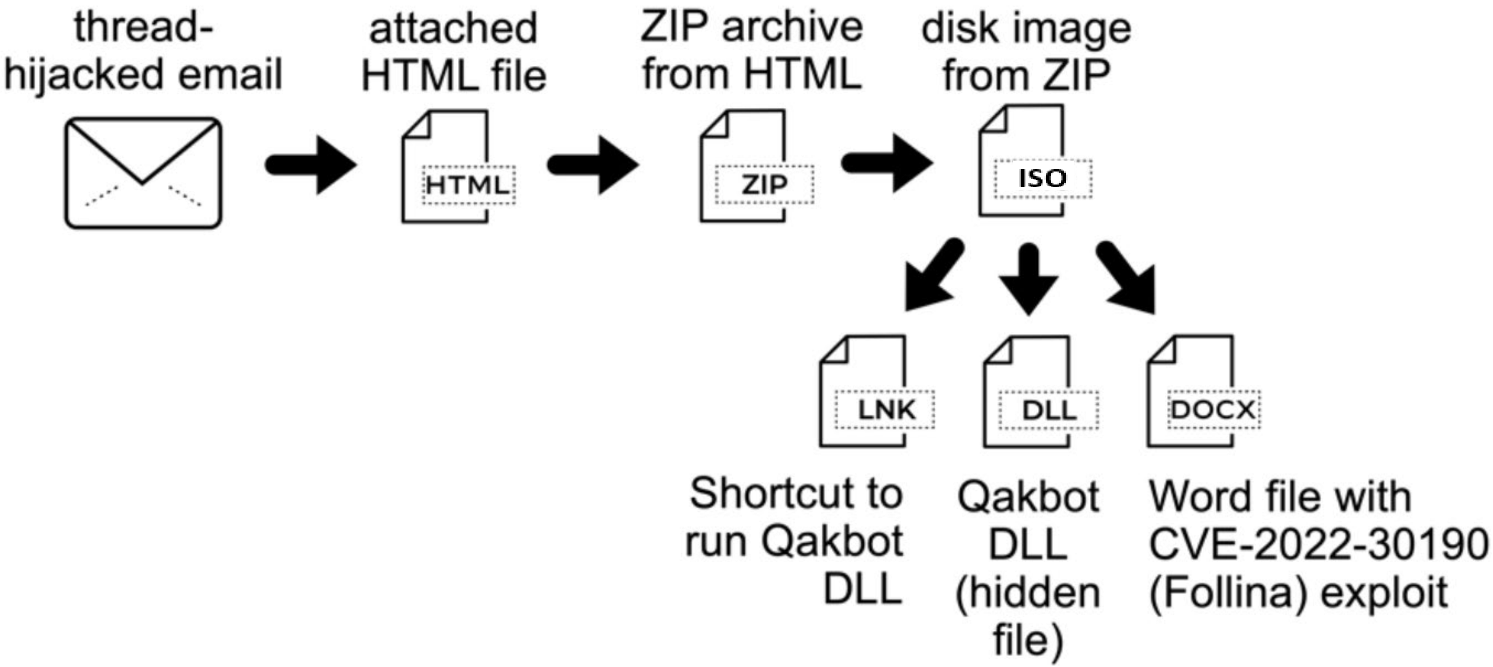
PDF reader | Adobe Acrobat Reader

This free PDF **reader** app lets you view, omment, fill out, and sign PDF forms to help you move through your workflow quickly and effi y.

https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwjy4sagmJ_8AhVJFdQBHY3OAxEYABADGgJvYQ&ae=2&ohost=www.google.com&cid=CAASJuRokbSmQNuTK23K

Malware!

Alternative Initial Access vector … (2)



thread-hijacked email

attached HTML file

ZIP archive from HTML

disk image from ZIP

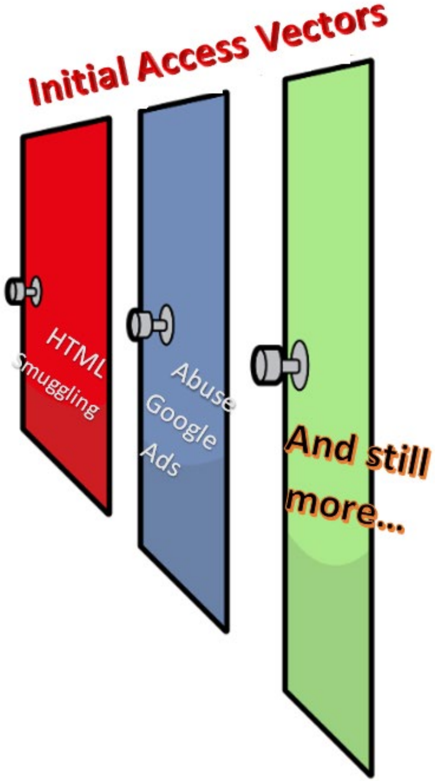
Shortcut to run Qakbot DLL

Qakbot DLL (hidden file)

Word file with CVE-2022-30190 (Follina) exploit

How to take advantage of this change?

Internet Macro Malwares
OLD
Threat Actor



Quick Takeaways:

1. Macro malware, as an easy Initial Access vector, is almost over.

2. Now, threat actors are seeking (new) alternatives to gain initial access.

3. The known attack surface will change.

Use of commercial pentest tools in most attacks

cobaltstrike

BRUTE RATEL

Use of OS built-in tools / programs in attacks

Living Off The Land Binaries, Scripts and Libraries

- Powershell.exe
- Certutil.exe
- Bitsadmin.exe
- Cmd.Exe
- Explorer.exe
- Mshta.exe
- Msiexec.exe
- Reg.exe
- Regedit.exe
- Regsvr32.exe
- Rundll32.exe
- Schtasks.exe
- Wmic.exe
- Wscript.exe
- Net.exe

- At.exe
- Cmstp.exe
- Mshtml.dll
- Ieframe.dll
- Setupapi.dll
- Shell32.dll
- Url.dll
- Zipfldr.dll
- Comsvcs.dll
- Cl_LoadAssembly.ps1
- CL_Invocation.ps1
- Pubprn.vbs
- UtilityFunctions.ps1
- Nltest.exe
- …

Quick Takeaways:

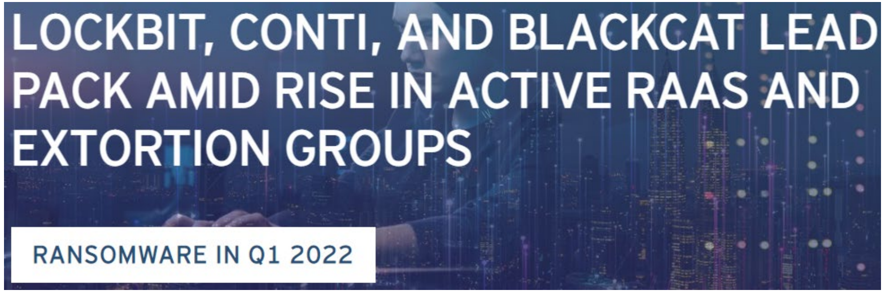
1. Commercial pentest tools lend threat actors efficiency and speed during an attack.

2. The use of OS built-in & normal tools complicates detection and response.

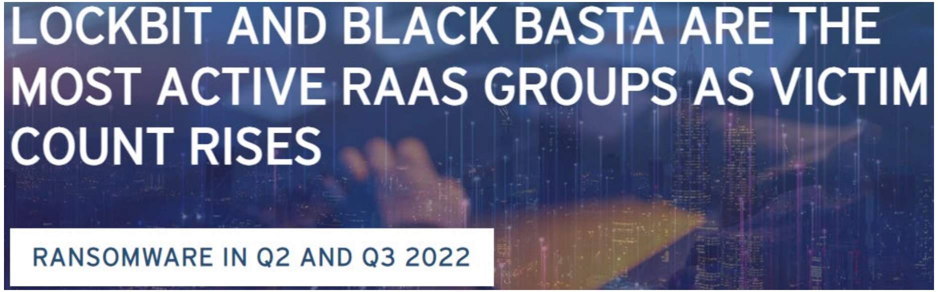
3. We are moving to less-malware-but-more-commercial/normal tools attack scenario.

Ransomware Landscape

TREND MICRO™


LOCKBIT, CONTI, AND BLACKCAT LEAD PACK AMID RISE IN ACTIVE RAAS AND EXTORTION GROUPS

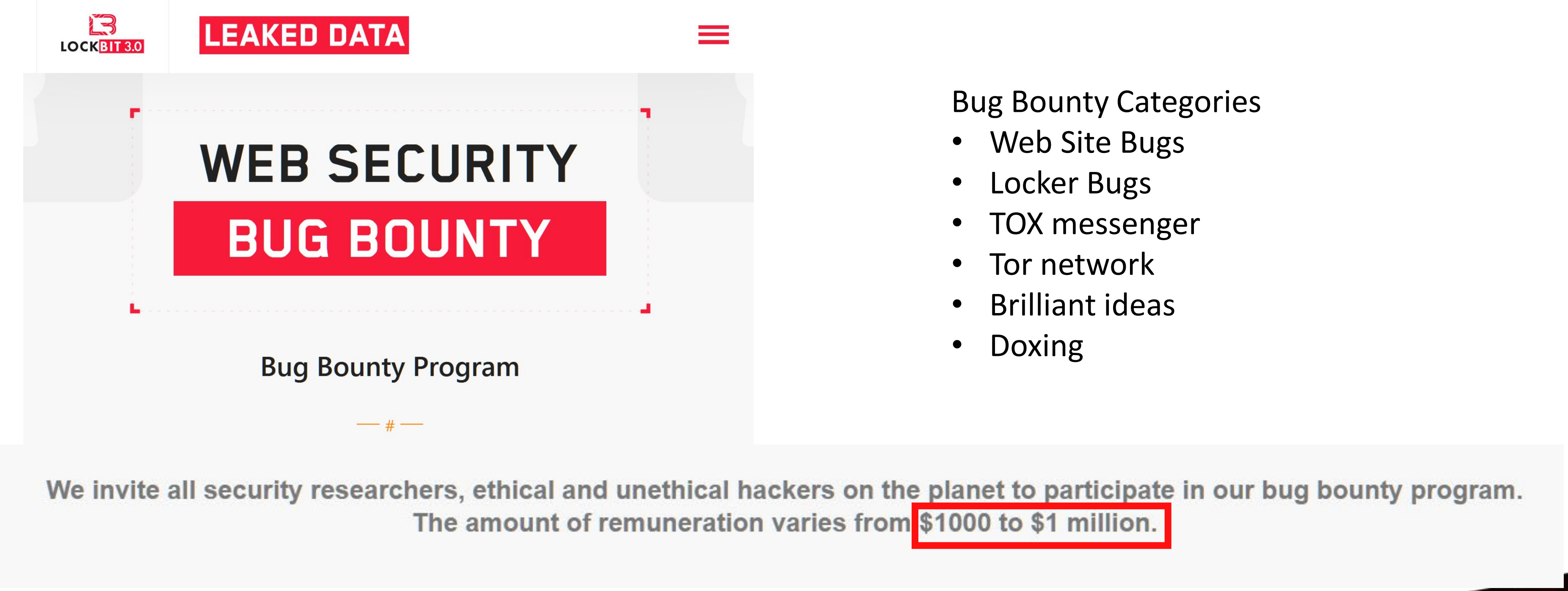
RANSOMWARE IN Q1 2022


LOCKBIT AND BLACK BASTA ARE THE MOST ACTIVE RAAS GROUPS AS VICTIM COUNT RISES

RANSOMWARE IN Q2 AND Q3 2022

Lockbit aka Water Selkie

LockBit 3.0 introduced the first ransomware bug bounty program



Bug Bounty Program

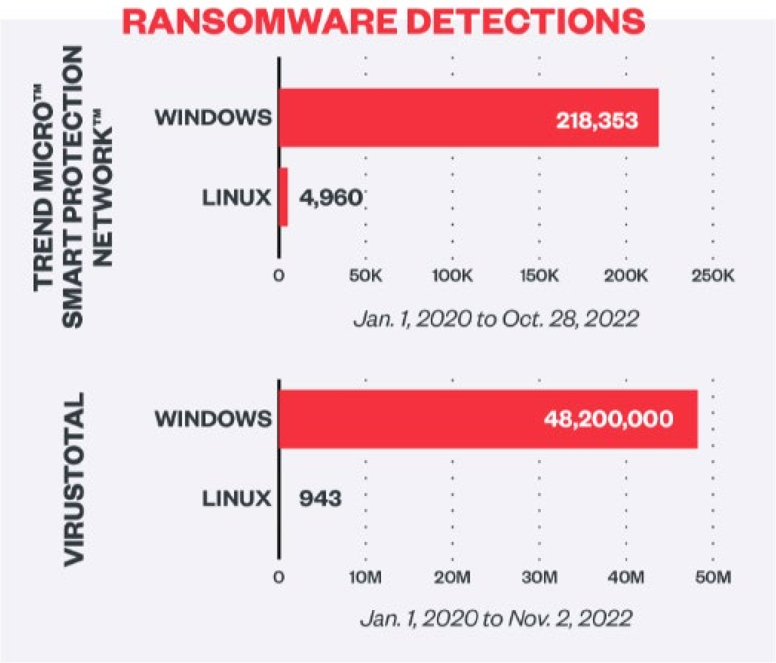
We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program. The amount of remuneration varies from $1000 to $1 million.

Bug Bounty Categories

- Web Site Bugs
- Locker Bugs
- TOX messenger
- Tor network
- Brilliant ideas
- Doxing

Source: Ransomware Spotlight Lockbit

Ransomware Linux-based Versions



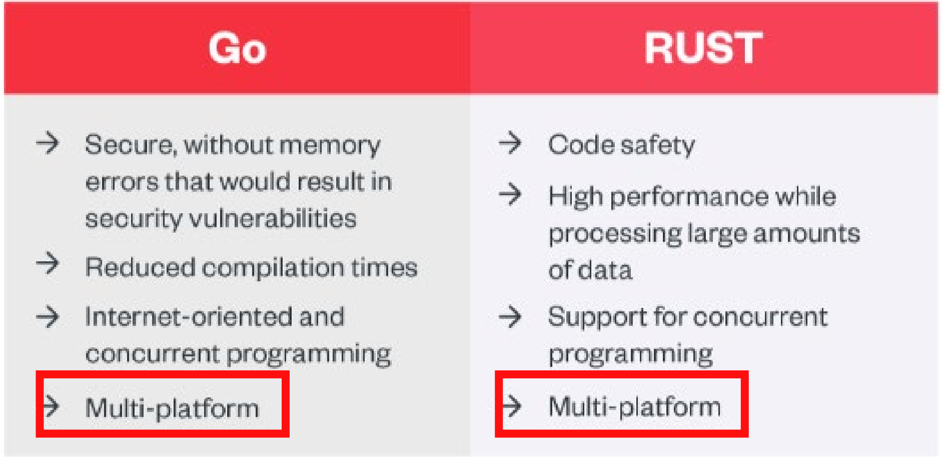
Perform more wide-spread attacks on targets using Linux-based servers

Ransomware Linux-based Versions

Groups shifting to Rust and Go eventually develop Linux variants

Ransomware	GoLang	Rust	Linux Variant
Hive	✓	✓	✓
BlackCat		✓	✓
Babuk	✓		✓
BlackByte	✓		✓
PartyTicket	✓		✓
Snatch	✓		✓
Decaf	✓		✓

Why adversaries switch to Rust and Go



Go	RUST
→ Secure, without memory errors that would result in security vulnerabilities → Reduced compilation times → Internet-oriented and concurrent programming → Multi-platform	→ Code safety → High performance while processing large amounts of data → Support for concurrent programming → Multi-platform

Near and Far Future of Ransomware Business Models

Evolution

1. **Change of targeted endpoints** - internet of things (IoT)/Linux

2. **Scale up** through increased professionalism and automation

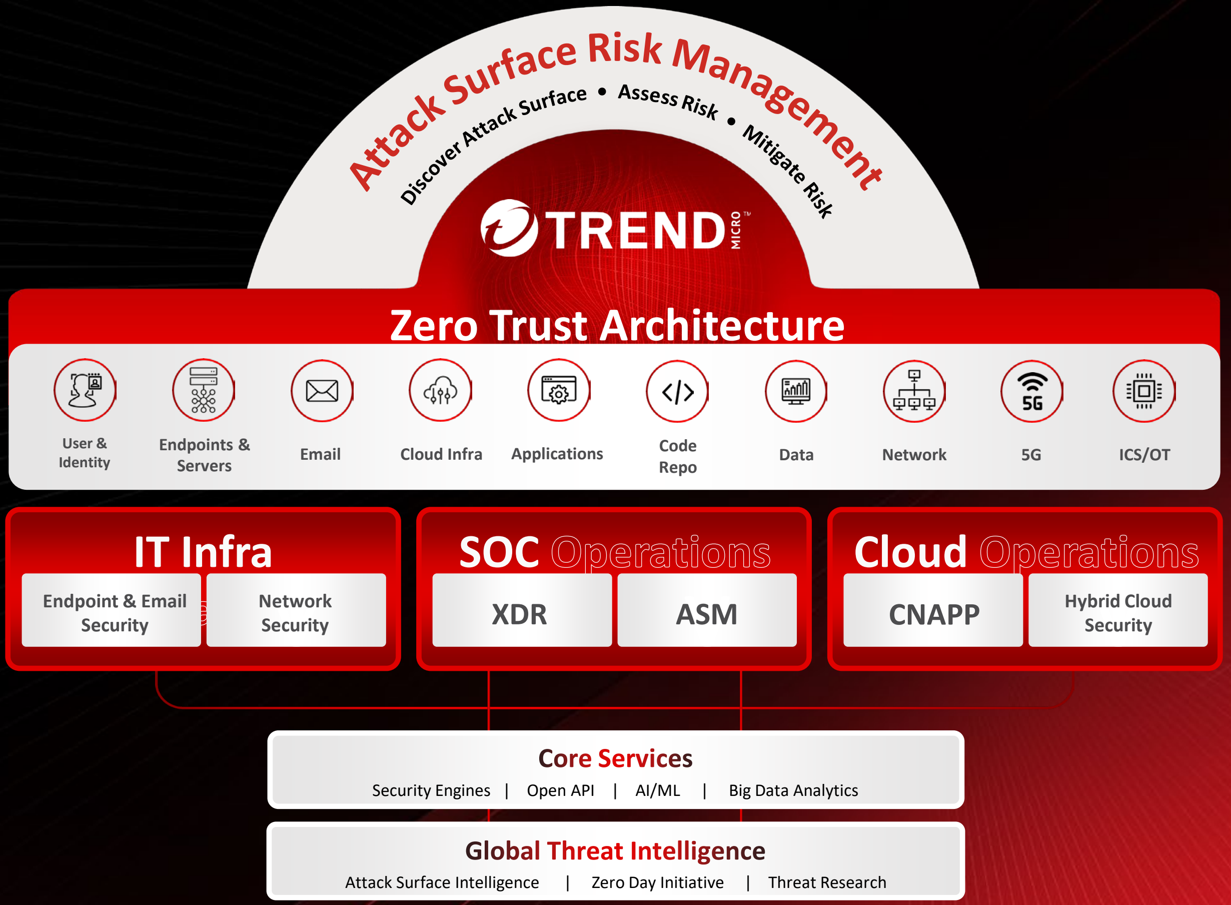
Revolution

1. Hack into **cryptocurrency** exchanges/Steal cryptocurrencies

2. Replace ransomware payload with **business email compromise** (BEC)

Trend Vision One XDR

Managed Services



Attack Surface Risk Management

Discover Attack Surface • Assess Risk • Mitigate Risk

TREND MICRO

Zero Trust Architecture

User & Identity | Endpoints & Servers | Email | Cloud Infra | Applications | Code Repo | Data | Network | 5G | ICS/OT

IT Infra

Endpoint & Email Security

Network Security

SOC Operations

XDR

ASM

Cloud Operations

CNAPP

Hybrid Cloud Security

Core Services

Security Engines | Open API | AI/ML | Big Data Analytics

Global Threat Intelligence

Attack Surface Intelligence | Zero Day Initiative | Threat Research

Ecosystem Integration

Bringing Simplicity to SOC Operations

TREND MICRO | research

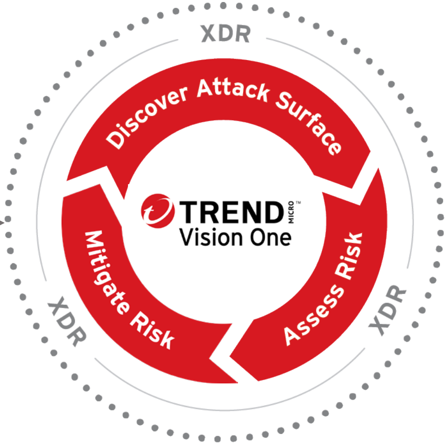
TREND MICRO SMART Protection Network™

ZERO DAY INITIATIVE

IOCs shared by:

Government Agencies
Security information sharing organizations
Independent Security Researchers
Third-Party Detections sourced from your SIEM
Corporate Security Teams
Other Security Vendors
Third-party TAXII/MISP

XDR Sensor Data (endpoint, email, network, etc.)



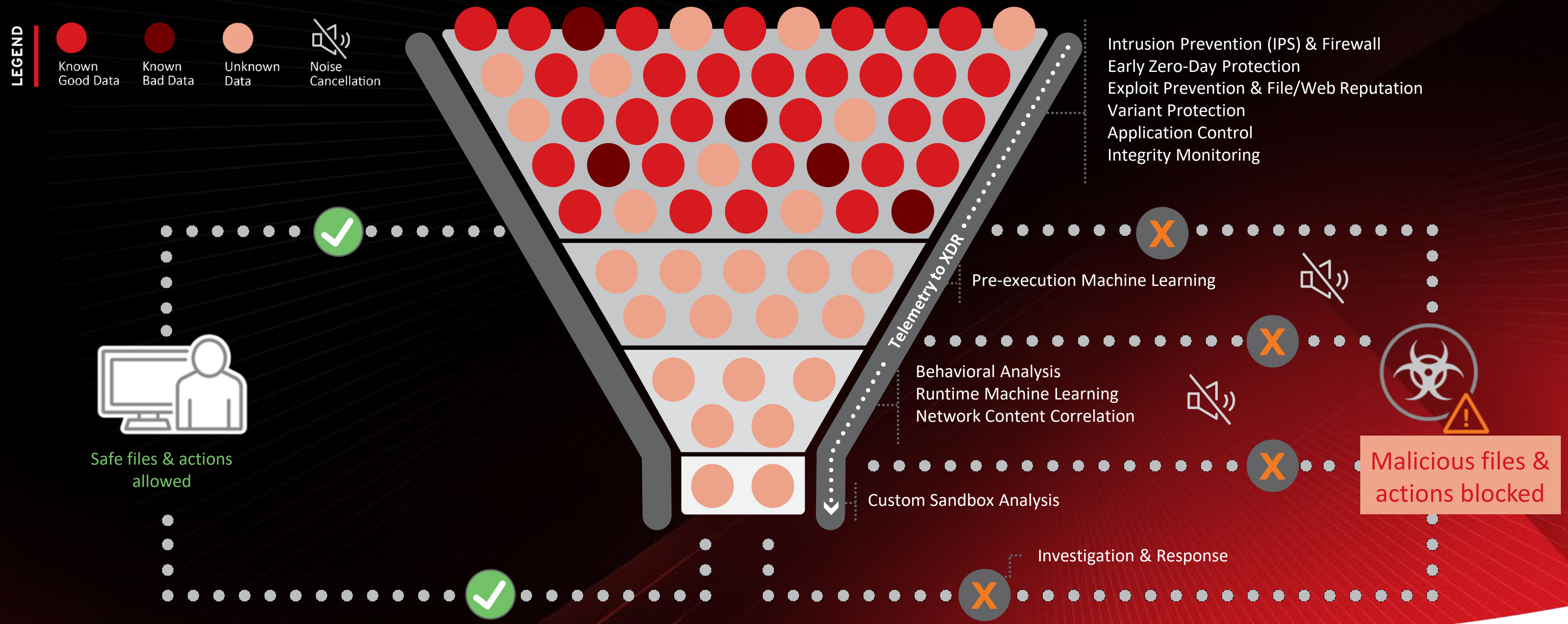
Centralized Risk Assessment
Centralized Investigation
Centralized Response
Centralized Cross-Vendor Block Lists

Automated or Manual Response

- Quarantine or Delete Emails
- User Password Reset or Disable Account
- Endpoint Isolation
- URL Blocking
- Network Firewall Rules
- Cloud Sandboxing

TREND MICRO

Smart, layered security maximizes protection



Intrusion Prevention (IPS) & Firewall
Early Zero-Day Protection
Exploit Prevention & File/Web Reputation
Variant Protection
Application Control
Integrity Monitoring

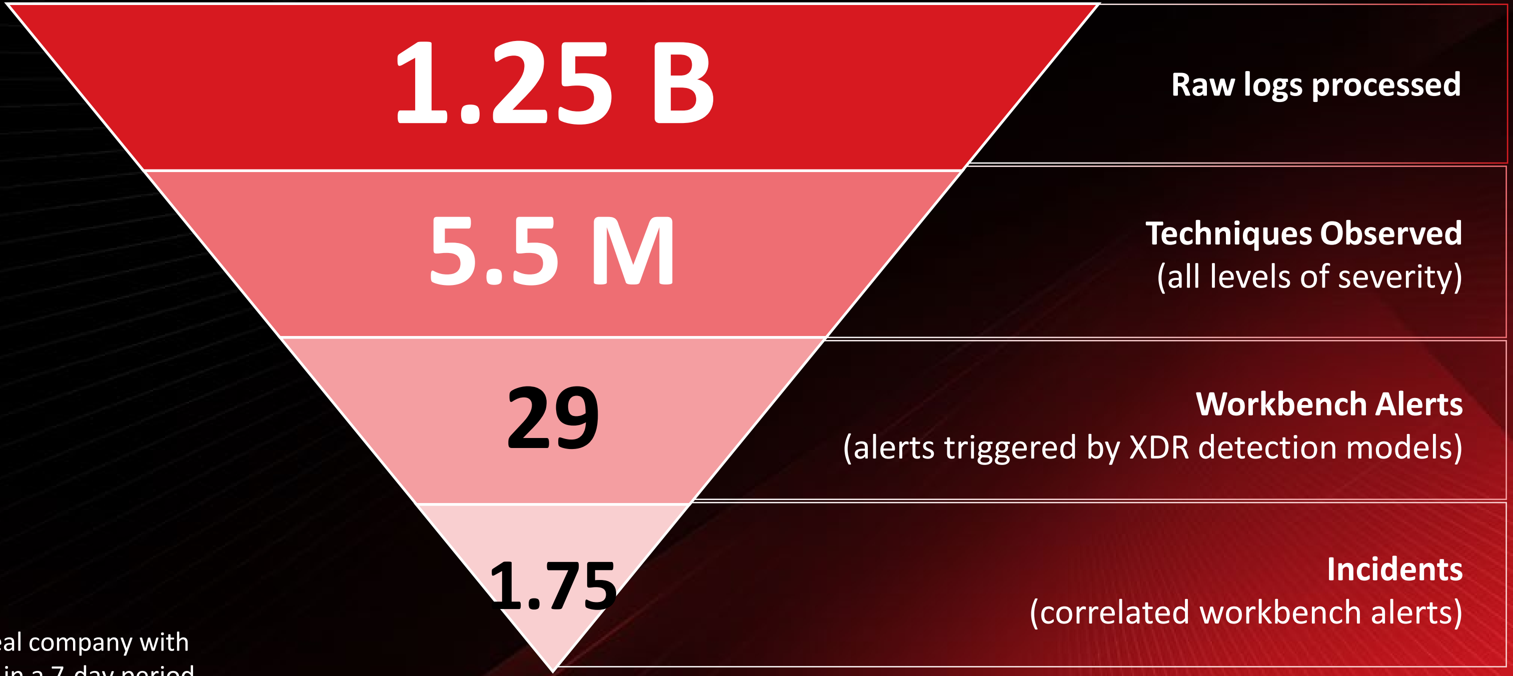
Pre-execution Machine Learning

Behavioral Analysis
Runtime Machine Learning
Network Content Correlation

Custom Sandbox Analysis

Investigation & Response

High Confidence Detections without Alert Overload



1.25 B — **Raw logs processed**

5.5 M — **Techniques Observed** (all levels of severity)

29 — **Workbench Alerts** (alerts triggered by XDR detection models)

1.75 — **Incidents** (correlated workbench alerts)

Based on a real company with
1000 devices in a 7-day period

Managed XDR: MDR Service by Trend Experts

Expert Threat Hunting
Cutting-edge techniques with verification and enrichment by threat experts

24x7 Monitoring & Detection
Continuous monitoring and routine sweeping of endpoint, server, network, and email

Rapid Investigation and Mitigation
Detailed response plan and remote actions through Trend Micro products

TREND MICRO™

“Big enough to deliver, small enough to care”

Thank you!