HORIZON3.ai

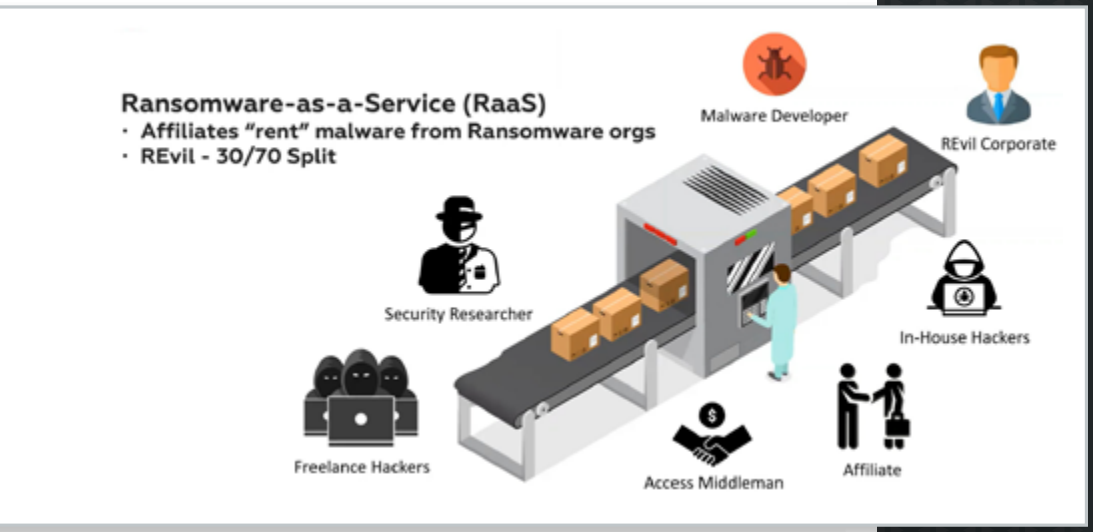
~~TRUST BUT~~ VERIFY

Ransomware Impact

with Horizon3

Ransomware is an increasingly common and lucrative attack, with organizations often paying millions of dollars to decrypt and recover their information. The 2021 Verizon Data Breach Investigation Report (DBIR) reported ransomware attacks are on the rise, "more than doubling its frequency[1]" from the previous year.

Ransomware attacks have become democratized, with criminal groups establishing Ransomware-as-a-Service (RaaS) operations, renting ransomware to recruited affiliates that, in turn, run attacks against organizations and pay a "royalty" to the RaaS providers.



Ransomware attacks are growing in prevalence and impact. How bad is it?

The US Treasury Department reported ransomware payments of **$590 million were paid in the first half of 2021**, more than the $416 million reported for all of 2020.[2]

A 2021 study by Sophos found that **37% of the respondents experienced ransomware attacks.** The average ransom paid by mid-sized organizations was $170,404.[3]

The 2021 attack on Colonial Pipeline by DarkSide shut down operations **until the company made a payment of $4.4 million**.[4]

CNA Financial, one of the largest insurance companies in the US, reportedly **paid hackers $40 million** after a ransomware attack blocked access to the company's network.[5]

Insurers offering cyber coverage have taken notice. AIG reported **raising its premium prices by 40%** globally.[6] Insurance provider Optio reported **reducing coverage limits by 50%.**[7]

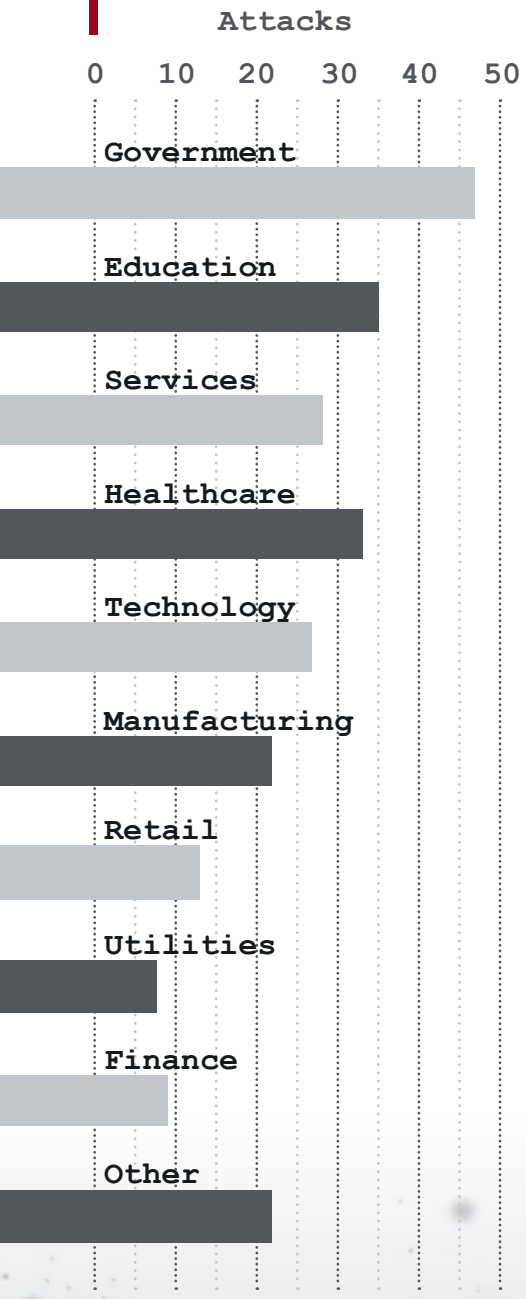
How Ransomware Works

In a ransomware attack, like a data theft attack, criminals infiltrate a company's network and then move laterally to identify sensitive business data. Initial access to the network often comes from compromising a legitimate credential. Instead of simply stealing a copy of the data, however, they encrypt it and demand payment in cryptocurrency before providing a decryption key. The recent BlackMatter ransomware attacks follow a common pattern.[8] Starting with a compromised credential, the ransomware conducts:

- **Active Directory Enumeration** – Captures information that can be used to discover hosts on the network, elevate privileges, or help with lateral movement.
- **SMB Share Enumeration** – Determines file shares that it can access with read/write privileges.
- **Credential Dumping** – Identifies hosts it has administrative access to and harvest more credentials from those hosts.
- **Encryption of SMB Shares** – This includes administrator-accessible shares like ADMIN$, C$, SYSVOL, NETLOGON.
- **Encryption of VMware ESXi Virtual Machines** – Criminals extend their attacks to include virtual machines.
- **Wiping/Reformatting** – Prevents organizations from rolling back systems to backup data stores and appliances.

Challenges Stopping Ransomware Attacks

RANSOMWARE ATTACKS BY INDUSTRY[9]



As one can see, ransomware attacks are similar to data theft attacks, but with a different treatment of the data (encryption). Unlike more sophisticated attacks, ransomware does not depend on long-term persistence on a network. The attack can be relatively quick and effective.

Organizations face several challenges defending against ransomware, including:

- **Simple attack vector** – Ransomware threat actors often rely on an ecosystem of initial access brokers who provide compromised credentials and web shells with access to the targeted organizations.
- **Unprotected or misconfigured systems accessible to unauthenticated persons** – For those not purchasing stolen credentials, finding a misconfigured or unpatched Internet-facing application can often provide an initial foothold.
- **Rapidly changing IT environment** – Organizations are constantly changing their environments. Moving to cloud hosting, shadow IT projects, and new applications all change the attack surface, making it difficult for defenders to identify, prioritize, and mitigate risk.
- **Non-scalable penetration testing** – Pentests can identify weaknesses and improve defenses. However, manual pentests are lengthy, costly, and incomplete.
- **Vulnerability scanners noise** – Some vulnerability scanner or penetration test report critical security findings. These require skilled analysts to determine if the reported findings are true positives, false positives, or worse, issues that require obtuse, highly unlikely sets of conditions to exploit.

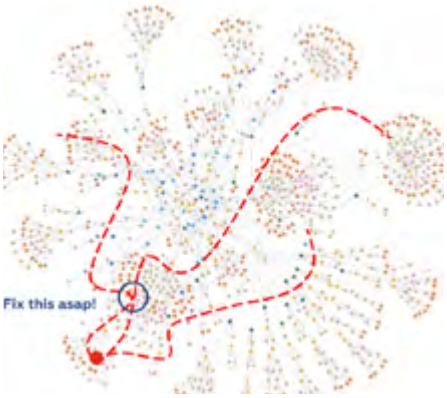
How Horizon3 Helps

NodeZero helps organizations understand the impact ransomware could have on their environments by using the same tactics and techniques used by skilled attackers. NodeZero identifies attack vectors, verifies the effectiveness of each, provides a "proof" to verify each weakness (or chain of weaknesses), enumerates all data and hosts it could compromise, and provides remediation guidance to eliminate the threat. Since it is an Autonomous Penetration Testing as a Service offering, pentests can start in minutes, not hours or days.

Reconnaissance – Like APTs, ransomware, and other threat actors, NodeZero conducts extensive reconnaissance to discover and fingerprint the internal and external attack surface, identifying the ways exploitable vulnerabilities, misconfigurations, harvested credentials, and dangerous product defaults can be chained together to facilitate a compromise.

Maneuver Loop – NodeZero acts as an Advanced Persistent Threat (APT), orchestrating over 100 offensive tools to harvest credentials, exploit vulnerabilities, and exploit default and misconfigurations to execute attacks.

Verified Attack Plans – The results are provided as "Proofs" with graphical and textual representations of each step of a successful attack, including tactics used, how credentials were obtained, paths taken to gain privileges and access to systems.



Impact – Like a determined attacker, NodeZero surfaces data at risk across physical and virtual environments it was able to access with read/write privileges, including SMB shares, NFS shares, FTP shares, cloud storage, vCenter servers, and databases.

Contextual Scoring – Instead of relying on CVSS scores, NodeZero evaluates each weakness by its role in the successful attack. Organizations can quickly identify those weaknesses that present the greatest threat and must be addressed immediately, and which weaknesses can be safely deferred.

Actionable Remediation – NodeZero provides precise and actionable remediation guidance, allowing security and operations to resolve issues at the root cause.

Ready to Learn More?

NodeZero is an Autonomous Penetration Testing as a Service (APTaaS) that helps organizations **find and fix attack vectors before attackers can exploit them**. It is safe to run in production and requires no persistent or credentialed agents.

- **Sign up for your free demo today.**

ARTICLE SOURCES[N] - https://www.horizon3.ai/ransomware-impact-sources

HORIZON3.ai
TRUST BUT VERIFY