imagine IT

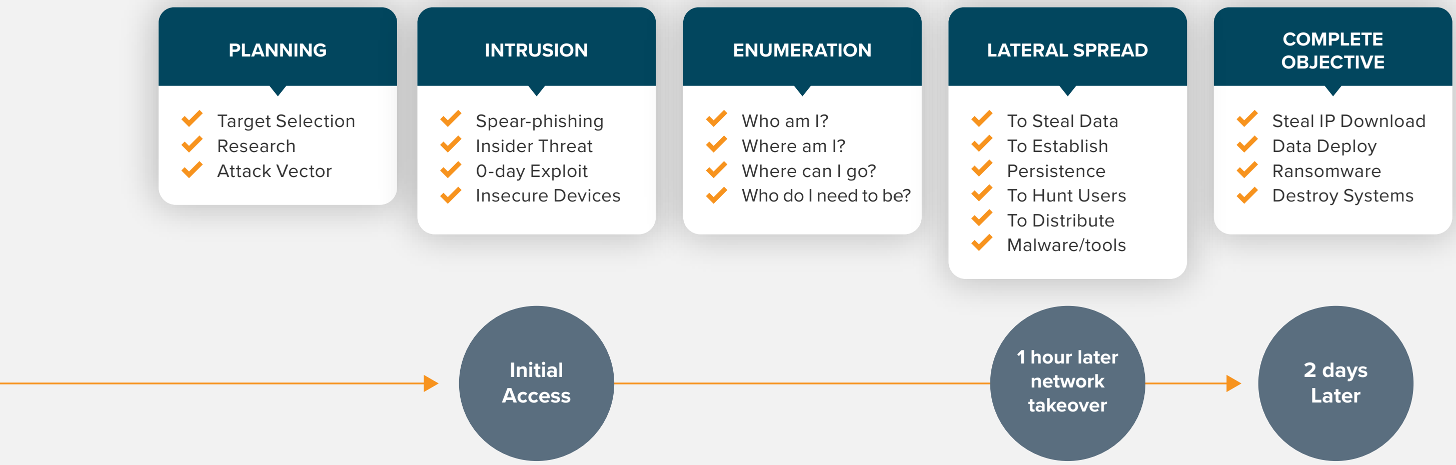
The Q3 2024 State of Cybersecurity

imagineiti.com

Only 1-hour from hacker initial access to network takeover

Over the last few years, the "Hacker Attack Chain" has evolved from a 200-day process down to a 2-day process...

Hacker Timeline



PLANNING

- ✓ Target Selection
- ✓ Research
- ✓ Attack Vector

INTRUSION

- ✓ Spear-phishing
- ✓ Insider Threat
- ✓ 0-day Exploit
- ✓ Insecure Devices

ENUMERATION

- ✓ Who am I?
- ✓ Where am I?
- ✓ Where can I go?
- ✓ Who do I need to be?

LATERAL SPREAD

- ✓ To Steal Data
- ✓ To Establish
- ✓ Persistence
- ✓ To Hunt Users
- ✓ To Distribute
- ✓ Malware/tools

COMPLETE OBJECTIVE

- ✓ Steal IP Download
- ✓ Data Deploy
- ✓ Ransomware
- ✓ Destroy Systems

Initial Access

1 hour later network takeover

2 days Later

How is it that hackers **can take control of the network 1-hour from initial access?** In the previous decade the hackers knew they could remain in victim systems for many months without being detected. They would use the victim networks to attack other victims, then eventually plant ransomware and/or steal intellectual property.

But in 2024 the cybercriminals know that the defenders are getting stronger, so they get in and out quickly. The attackers now have at their disposal more weapons to assist with rapid exploitations...

Automated Tools Shared on the Dark Web

Hackers use sophisticated automated tools that can quickly exploit vulnerabilities and move laterally within a network or cloud and elevate privileges.

AI Generated Phishing and Social Engineering

These methods allow attackers to gain initial access by tricking employees into revealing credentials or clicking on malicious links.

Exploiting Known Vulnerabilities

Attackers often exploit unpatched software vulnerabilities to gain access and elevate privileges.

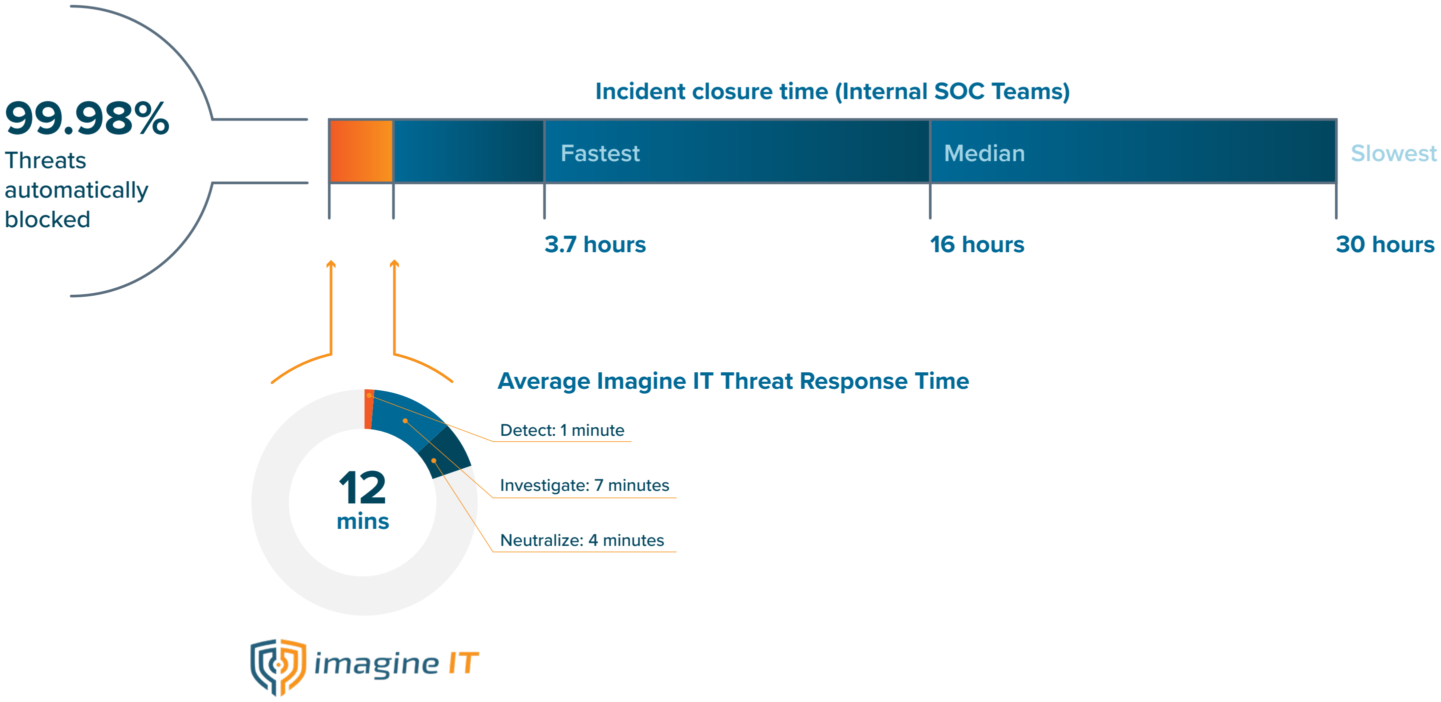
Ransomware-as-a-Service

This cybercriminal business model is sold to less skilled hackers, allowing them the ability to launch effective attacks using pre-built kits.

These factors combined enable hackers to move swiftly from initial access to full network control, often in less than an hour. This gives defenders very little time to detect, analyze, and neutralize threats.

Why 15 minutes from threat detection to neutralization is critical

Considering the new speed of attack, orgs MUST be able to neutralize threats within 15 minutes of detection. Unfortunately, very few orgs have this capability.



Notice that the typical Security Operations Center (SOC) averages 16 hours from detection to neutralization. This is MUCH too slow and will result in confidential data exfiltration and ransomware.

Here are some key reasons why fast neutralization is critical:

Containment of Damage

The faster a threat is neutralized, the less time it has to cause harm. This includes preventing data breaches, system disruptions, and unauthorized access.

Cost Reduction

Quick response times can significantly reduce the financial impact of a cyber-attack. The longer a threat remains active, the higher the costs associated with containment, recovery, and potential fines.

Protection of Reputation

Swift action helps maintain customer trust and protects the organization's reputation. Delays in response can lead to public relations issues and loss of customer confidence.

Compliance

Many regulatory frameworks require timely incident response. Meeting these requirements helps avoid legal penalties and ensures the organization remains compliant with industry standards.

Operational Continuity

Rapid threat neutralization ensures that business operations can continue with minimal disruption, maintaining productivity and service delivery.

Bottom line, defenders MUST kick intruders out before the cybercriminals laterally spread across the systems. This includes premise systems, and cloud systems like Microsoft 365 and Google Workspace.

Are we too small to be a target?

Many executives hold a dangerous mindset that they are too small to be a target. Truth be told, they are not too small to be a target, just too small to make the news.

SMBs are 4x more likely to be a victim than large orgs. Why? The perception and reality is that small and medium businesses lack the budgets and skillsets to properly defend and respond to cyber-attacks.

Why do criminals like Small Businesses?

Using thrid
party software

No IT deparment

Big data

Less likely to
follow internet
best practices

Using the
Cloud

Easy target

Simple networks
& systems

Small businesses are often targeted by cybercriminals for several reasons:

Limited Resources

Small businesses typically lack the extensive cybersecurity infrastructure that larger companies have. This makes them easier targets for cybercriminals.

Valuable Data

Despite their size, small businesses often hold valuable data, such as customer information, payment details, and intellectual property, which can be lucrative for cybercriminals.

Perceived Easier Targets

Cybercriminals often view small businesses as easier targets because they assume these businesses are less likely to have robust security measures in place.

Lack of Awareness

Many small business owners may not fully understand the risks or may underestimate the likelihood of being targeted, leading to insufficient cybersecurity practices.

Financial Gain

Attacks on small businesses can still yield significant financial rewards for cybercriminals, whether through direct theft, ransomware, or selling stolen data.

It's crucial for small businesses to invest in cybersecurity measures that protect the business mission. Detection & Response is a great starting point.

Conclusion

Any organization with a bank account or intellectual property is a target for cybercriminals and rogue nation-states.

Orgs MUST assume at some point a hacker will obtain initial access, and therefore MUST have the capability to neutralize the attack within 15 minutes. If your org does not possess this capability, or if you are unsure, please reach out to an IT Managed Service Provider that specializes in Cybersecurity, like Imagine IT.