IMAGINE IT

The Q3 2022 State of Cybersecurity

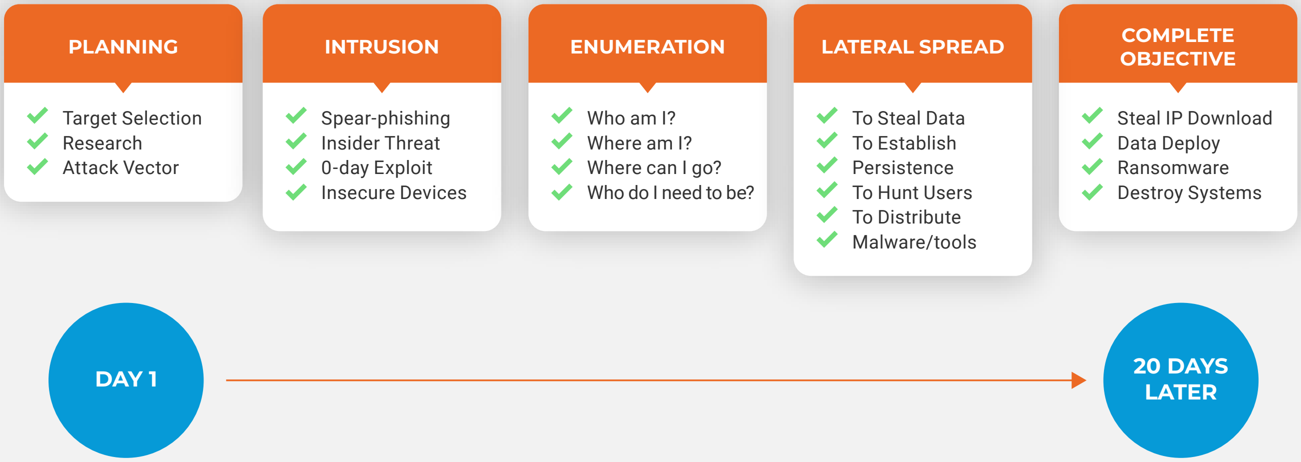
imagineiti.com

UNDERSTANDING THE HACKER TIMELINE

What is the process hackers follow to obtain access to business data?

The world has changed, and traditional security technologies like firewalls, antivirus, VPNs, and passwords are no longer enough. Breach tools have become widespread and commoditized, and it's now just too easy for cyber-criminals to gain a foothold in business environments. Here is how hackers successfully compromise businesses...

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

Planning

Hackers rarely blast out phishing emails en masse. Instead, they have found it significantly more successful to perform targeted attacks. They will:

- Select a target org.
- Check the website “about us” page for names and roles.
- Scan the Dark Web for any breach information; there will be some of it for sale.
- Use a Search Engine to obtain all other information about the org.
- Determine which publicly known vulnerabilities and 0-day exploits to utilize.
- Finalize the attack plan.

Intrusion

When the Hacker starts executing the attack, they will:

- Scan the firewall and what the firewall allows exposure to inside the network.
- Send spear-phishing emails (very targeted).
- Expose the targeted users to the known vulnerabilities and 0-day exploits.

Once the hacker succeeds (all orgs MUST assume this will happen at some point) they will move on to the next phase...

Enumeration

After initial intrusion the Hacker will:

- Determine what permissions they have.
- Analyze what data is available to compromise.
- Attempt to elevate permissions to an Admin level (they will likely succeed at this).

It is critical that the org detect the Hacker during this phase. ALL breaches you hear about happened largely because the targeted org had insufficient “Detection” technologies in place, and the hacker was able to roam about freely until they achieved their objective.

Lateral Spread

Unfortunately, computer networks (Windows, Mac, & Linux) were designed long ago to allow sharing of information and printing. Hackers take advantage of this and utilize easily exploitable vulnerabilities in networks to:

- Move from one computer to another.
- Establish hidden persistence.
- Spread malware.

Once Lateral Spread is complete it is pretty much game over. Be aware there are modern network management platforms that make it much more difficult to perform Lateral Spread.

Complete Objective

There are 3 common objectives, and they are often used in tandem:

1. Steal Intellectual Property. This is a common goal of Nation State and Politically Motivated attackers, and they will try to never make their presence known.

2. Download all available data. This is typically a precursor to Ransomware.
3. Launch Ransomware. At this point the org better have a well-tested Backup & Recovery system, a well-rehearsed Incident Response Plan, and a comprehensive Cyber Insurance policy.

WHAT YOU CAN DO TO PROTECT YOUR ORG

The 4 Key Takeaways from The Hacker Timeline:

1. Deploy modern PROTECTION technologies that block attacks.
2. Deploy modern DETECTION technologies to become aware of intruders.
3. Annually rehearse the INCIDENT Response Plan with your IT Managed Service Provider (MSP) so your org can kick out intruders before they complete their objective.
4. Migrate to a modern network management platform to thwart Lateral Spread.

A comprehensive cybersecurity strategy will encompass more than this, but these takeaways will go a long way. Engage with your MSP.

What's Around The Corner?

24/7 Security Monitoring & Remediation

Most security protection and detection technologies "notify" IT staff of things to investigate. On the surface this seems fine, however...

- These technologies typically do not "remediate" the threat.
- IT support staff are not skilled enough to understand the alerts nor how to quickly remediate them.
- There is an immense amount of alert "noise", wasting IT staff time reviewing false positives and allowing true positives to slip through the cracks.
- IT staff typically work regular business hours. What happens when a critical alert comes in at 2a?

Imagine IT customers enrolled in our Security Shield "Basic" program utilize a Threat Hunting tool that can auto-isolate a compromised computer 24/7. However, it is only automated, and there are no 24/7 "human-led" investigations. Without human-lead Threat Hunting and investigation, a hacker could sneak by.

Imagine IT customers enrolled in our Security Shield "247" program utilize both an automated and a 24/7 human-led Threat Hunting system. These human-led teams have the authority to perform remediation on behalf of the MSP. And if an optional Network Sensor is deployed, suspicious activity can be correlated between network traffic AND the computers.

Peter's Insight

Most breaches happen overnight. Therefore, it is critical to detect and kick out intruders 24/7 BEFORE they laterally spread and complete their objective.

Security pro-tip of the quarter

Cell Phone App Security

Cell phones are small but powerful computers. Your cell phone is millions of times more powerful than the 1960's computers that sent humans to the moon. Amazing! And cell phones can download and run millions of apps. But how do you know the apps are safe?

You may have heard of "supply chain attacks". This is often the result of a software application utilized by the business that gets infected in the providers environment. For example, your main line of business or accounting software manufacturer pushes out an update, but the update has been pre-infected by an attacker, thereby infecting YOUR network.

How does this pertain to cell phones? Every single app on your cell phone is susceptible to Supply Chain Attacks, and you have little or no way to detect or block them. And if you become a victim, you risk the business and you risk identify theft and your privacy.

The best you can do is to reduce the attack surface...

- Remove and/or not deploy entertainment or unnecessary apps and tools.
- Only use your cell phone for its core functions: calls, texts, messaging, email, GPS mapping, etc...
- Move entertainment and non-critical apps to a tablet that is not tied to messaging and email.

You will start hearing about cell phone supply chain attacks more and more, so please try to avoid being a victim.

Conclusion

It is critical to detect hackers BEFORE they laterally spread and achieve their objective. Talk to your MSP and ask them to prove these DETECTION technologies are in place.