NEXUS IT
CONSULTANTS

HACK THE HACKER

An in-depth look into the hacker's playbook

Key Concepts

NEXUS IT
CONSULTANTS

Attack Vector: The point of weakness the bad guys attack

Ransomware: Code used to silently encrypt irreplaceable data, pay to unlock

Phishing: Fraudulent emails purporting to be from reputable companies used to induce employees to reveal personal information (passwords and credit card numbers)

Spear Phishing: The same as phishing, except the email comes from a ‘known sender’

Worm: A hallmark of ransomwares. Worms spread autonomously through networking vulnerabilities. Could be considered ‘phase 2’ of more sophisticated attacks.

Who's Attacking Me?

1. **Organized Crime** *(Think Tony Soprano)*
2. **Nation States** *(Russia, North Korea, China, etc)*
3. **Hacktivists** *(Anonymous, Shadow Brokers)*
4. **Lone-Wolves** *(Intelligent, financially driven, unscrupulous)*
5. **Malicious Insiders** *(Disgruntled employee/contractor)*

All of these types of hackers must be considered a threat, as a big part of their operations include funding for future attacks. That's why attacks like ransomware are becoming so prevalent!

Attack Vectors Explained

1. **Physical** – Theft, malicious USB drives, unsecured workstations

2. **Endpoint** – Remote attacks on vulnerable workstations

3. **Mobile** – Exploitation of iOS and Android – growing in prevelance

4. **Cloud** – Attacks on cloud solutions such as AWS, Azure

5. **IoT** – Stands for ‘Internet of Things’. Exploitations of devices like security cameras

Attack Vectors Explained

Physical

Cloud

NEXUS IT
CONSULTANTS

The “Human Attack Vector”

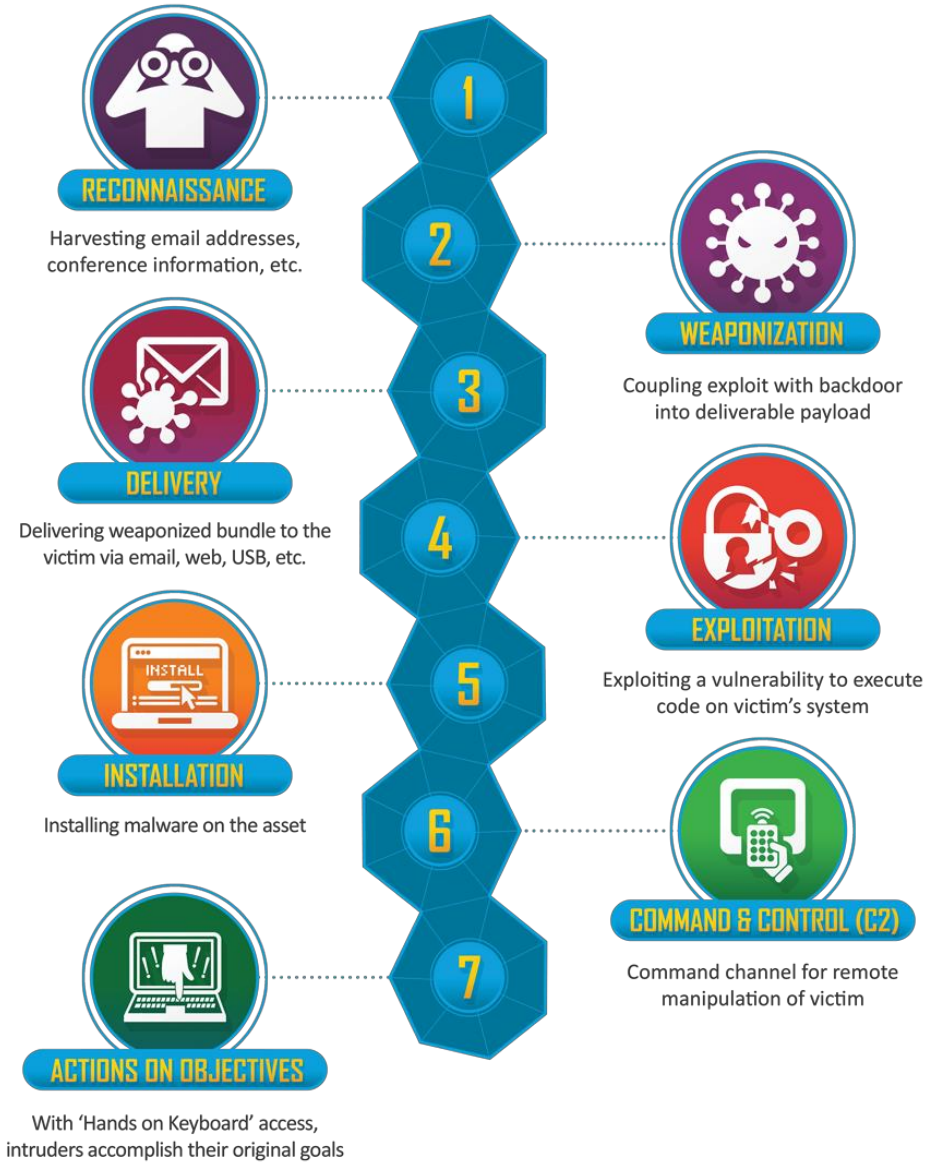
NEXUS IT
CONSULTANTS

Statement: Attackers go for the most vulnerable point of attack – humans (98% of all attacks are social engineering)

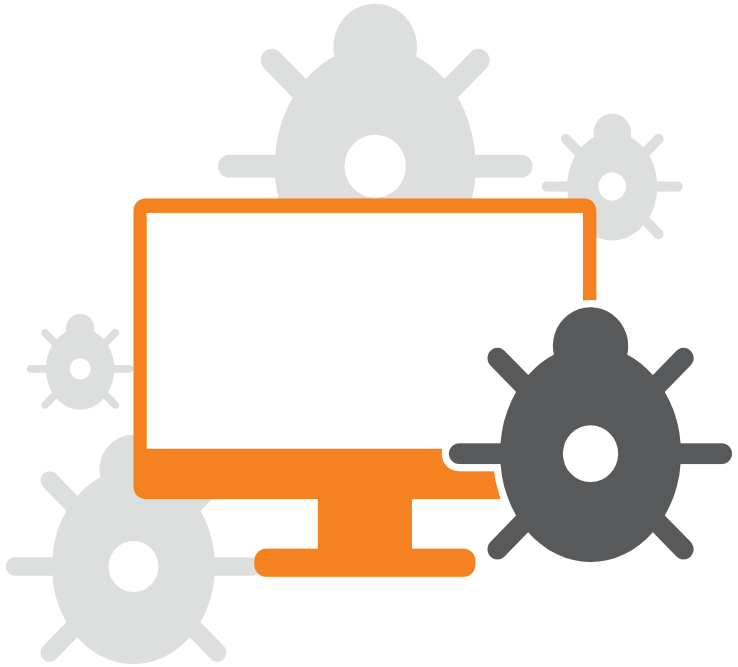
FALSE – Attacks are becoming more sophisticated in how they deliver malicious code, but here’s what is true:

Humans are involved In nearly 100% of all initiations.

What exactly does that mean? Let’s look at something Called the ‘Kill Chain’:



NEXUS IT
CONSULTANTS



The Anatomy of a malicious Email

NEXUS IT CONSULTANTS

Email is the easiest method of delivery in the kill chain. Hackers who use this approach are casting a very wide net and hoping for a relatively low rate of infection

- Remember – Humans are involved in almost all initiations

- Learning to identify fraudulent email is essential for every employee – technical or not!

The Anatomy of a “Spoofed URL”

NEXUS IT CONSULTANTS

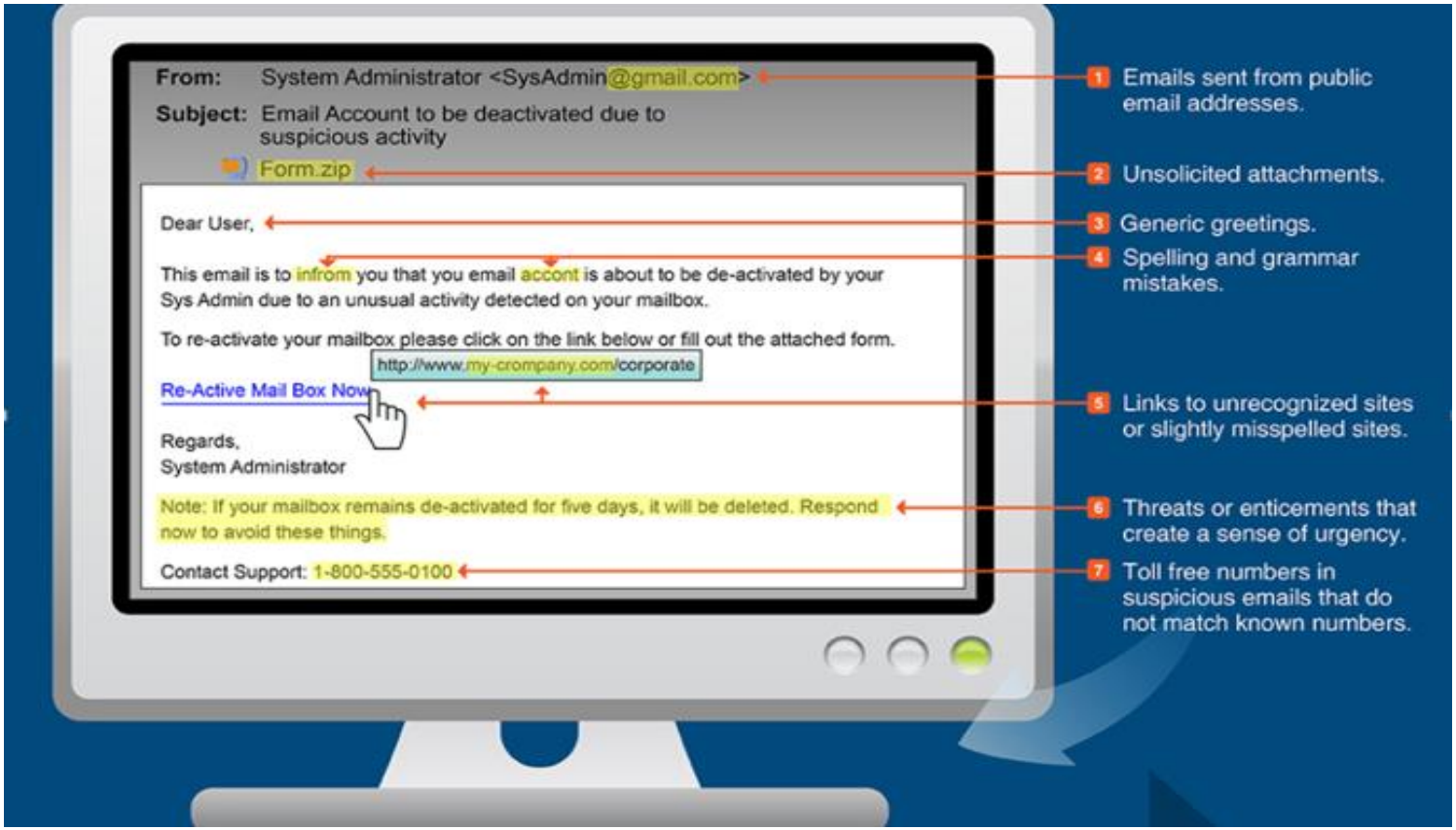
Email scammers will try to create a sense of urgency.

This is done by sending emails implying that not clicking a link will have severe negative consequences, like having your bank account frozen.

If a bank or another institution has an urgent message for you, it should also be available when you log directly into your account or get in touch over the phone. (Go straight to the source!)

The Anatomy of a malicious Email

NEXUS IT CONSULTANTS



The Anatomy of a “Spoofed URL”

NEXUS IT CONSULTANTS

Always ensure the following to stay safe:

1. Look Before You Click – Hover over any links and investigate before you click!
2. Check for Subtle Tricks – Scammers will use slightly misspelled variations of well-known sites to trick you into simply skimming the URL and clicking.
3. Be Wary of URL Shorteners

http://www.ksl.com http://www.udot.com/ http://goo.gl/ywXi3m

Worm-Based Exploits

Worms are network-based, self-replicating attacks.

They spread without human interaction once the first machine is infected on a network

Before widespread use of networks, computer worms were spread through infected storage media, such as floppy disks

A great example of the evolution of the hacker –

Physical attacks have been replaced by virtual attacks!

Worm-Based Exploits

NEXUS IT CONSULTANTS

THE GOOD NEWS: Worms often use legacy vulnerabilities such as SMBv1 and can easily be remedied with active patching and the proper endpoint protection

It's much easier to contract a firm to patch a healthy system Than it is to bring them in for a messy cleanup!

WannaCry - A Case Study

We've talked about Ransomware, and Worms, let's look at how they wreak havoc together using one of the most infamous examples; WannaCry:

WannaCry gets all the glory, but it was just the "Payload"

A payload is simply the weaponized part of the kill chain – step 2

EternalBlue is the real workhorse behind the rapid spread of WannaCry

EternalBlue was a known NSA exploit that was stolen by a Hacktivist group called "Shadow Brokers" on April 14, 2017.

EternalBlue was the delivery mechanism that delivered the WannaCry Ransomware payload. **And it was delivered without any human interaction!**

WannaCry - A Case Study

WannaCry started infecting machines on May 12th, 2017 (one month after it was stolen from the NSA)

Microsoft is purported to have known about the exploit and was working on a fix in the background

Microsoft issued a patch on May 13th, 2017

The weaponization of the stolen information was very quick. WannaCry highlights the most important aspect of Cyber Defense: Defense is inherently reactive

Success lies in being proactive!

Best Practices - Review

- ❑ Hover over addresses in emails and on webpages. Inspect the actual URL.
- ❑ Utilize all physical security measures that are reasonable
  - ❑ Lock computer screens when walking away
  - ❑ Workstation autolock settings enabled
  - ❑ No unauthorized personnel allowed to use PCs
  - ❑ If passwords are written down, lock them up!
- ❑ Know your source
  - ❑ Go straight to FedEx to retrieve that invoice rather than clicking on links
  - ❑ udot.scamsite.com is not the same as udot.com!
  - ❑ Link shorteners could go ANYWHERE – **hover and inspect!**
  - ❑ Don’t plug in USB devices you don’t recognize
- ❑ Ensure all systems are patched, up-to-date and protected against malicious code
  - ❑ The best systems recognize brand-new malicious code **based on it’s behavior!**

What If I Suffer An Infection/Breach?

NEXUS IT CONSULTANTS

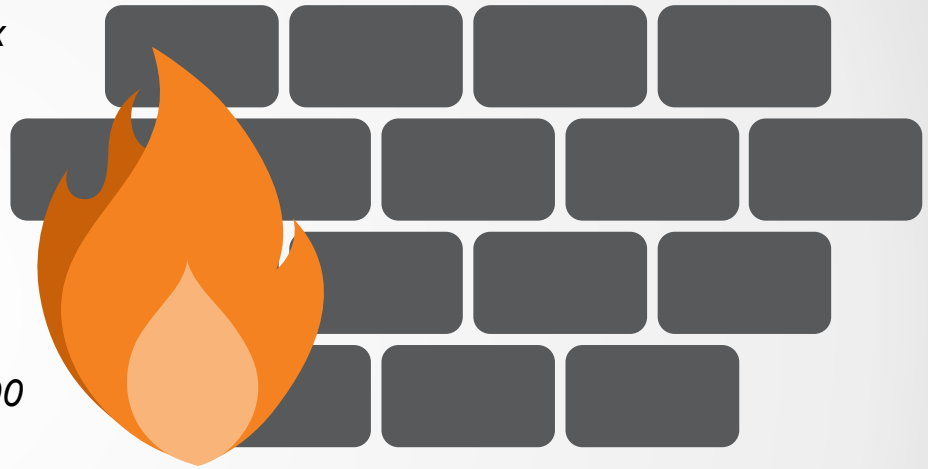
1. Immediately STOP, disconnect any potentially infected/breached devices from ALL networks
2. Change passwords to any potentially breached accounts
3. Call a Cyber Security Professional to begin forensic and remediation of the issue, **without destroying any data, information or evidence**
4. Call your Cyber Security Attorney
5. Call your Cyber Security Insurance Broker
6. Schedule a conference call with all of the above parties to determine best course of action and next steps

So How Do You Protect Yourself?

NEXUS IT
CONSULTANTS

So How Do You Protect Yourself?

- *Penetration Testing/Threat Assessment*
- *Solid UTM (unified threat management), not just random haphazard security solutions*
- *Commercial Grade Firewall (Not one you might buy at a big box store)*
- *Spam filtering*
- *Content Filtering - Control what web sites employees are accessing*
- *Lock down the use of 3rd-party cloud apps (Dropbox, etc…)*
- *Implement a mobile device policy and security protocols*
- *Force passwords that are difficult to hack, force change every 90 days*
- *Lock down user/admin privileges*
- *Back up and image your systems properly (protects against a number of threats)*
- *Employee education*
- *AUP (Acceptable Use Policy)*
- *Lock down the ability for employees to use home PCs and devices to access your network and cloud applications*



NEXUS IT
CONSULTANTS

Bottom Line:

You Need To Get Serious About Protecting Your Company Against Cybercrime and Cyber Threats!

But What Does That Look Like?

3 Steps To Protecting Your Organization:

Step 1: Threat Assessment

What's lacking in your security right now? How are employees using your company-owned devices? What 3rd-party cloud apps are you using? Are your systems truly backed up? Where are you exposed to risk? Whose job is it to make sure your network is protected, and how do you know if they're doing their job?

Step 2: Action Plan

Based on what's discovered, what do we need to do to ensure our systems, data and operations are secure from theft, compromise, corruption, etc.?

Step 3: Ongoing Monitoring/Maintenance

You definitely don't want to take a "set-it-and-forget-it" approach to security – your would-be attackers ARE NOT!

NEXUS IT
CONSULTANTS

Contact Us

https://www.nexusitc.net
support@nexusitc.net
435.487.9099

Timothy Sanborn
Partner Satisfaction Concierge
Microsoft & CompTIA Certified Technical Trainer with 11 IT Certifications