CYBERCRIME
BEHIND THE SCENES

THE EVOLUTION OF CYBERCRIME

With a technology revolution that has more and more applications being accessed in the cloud, and the ability to store or run applications in a hosted environment, even novice hackers have begun paying attention and leveraging this evolution to expedite their processes.

Originally, cybercrime was centralized – you had to build it from scratch. You couldn't call Rackspace to spin up some new servers, you had to do it all yourself. You had to identify the vulnerabilities and write the software for the attack. The entire process was very expensive. Because of the cost, the targets were larger customers who you could get the most money from.

Today it’s very different, it’s much more distributed. You can buy the different components to launch your attack and you can specialize in certain areas of the attack. It’s much cheaper and you can be much more opportunistic and target the much smaller and more vulnerable companies. Today, we’re seeing entire eco-systems around Cybercrime.

EASE AND ACCESSIBILITY

As cybercriminals have created their own eco-system, they have made cybercrime easier and more accessible to the general public. They have organized marketplaces where they can post opportunities for jobs or sell their tools to one another while leveraging their own unique finance solutions and payment systems for Bit Coin, an untraceable currency. With all of these advances, it is no longer only large corporations that are at risk, but small businesses are now in their cross hairs.

TARGETS ON SMALL BUSINESSES

As cybercrime advances and enterprises learn from their past mistakes, small businesses are increasingly targeted as they are viewed as newer and more flush with cash. Typically, they’re not actively managing security threats. Symantec, an antivirus company, sponsored a study that found that 41% of cyberattacks focused on small businesses. A separate Verizon study claimed that a company of 11-100 employees are 15 times more likely to be seriously breached.

TACTICS FOR INFECTION

The most common method of infection is a cleverly disguised email or advertisement. Since creating these attacks is cheap, or even free, cybercriminals spend their time producing higher quality material, leveraging logos and recognizable names to trick users to click on links that redirect to inadvertently download an exploit kit. Once downloaded, this exploit kit allows the cybercriminals to install malware onto the users computer. At times, attackers will sell the “infection rights” on the online marketplace, so that another attacker can carry out their infection plan without having to implement the initial infection.

CONCLUSION

While this information is indeed scary, it is not meant to scare you, but to inform you of what is going on behind closed doors. Talk with your IT provider for more information on what is being done to protect your business and what other measures that can be taken to prevent these malicious attacks.

INFECT

- Finely Tuned Emails
- Targeted Malvertising
- Exploit Kits

EXPLOIT

- Dropper Malware
- Malware Payload
- Keyloggers
- Ransomware
- CryptoVirus

PREVENT

- Block Exploit Kits
- Protect from Phishing
- Block Malicious Links
- Prevent Droppers
- Stop Virus Uploads
- Layered Security
- Stay Alert

11551 Nuckols Rd, Suite H, Glen Allen, VA 23059
☎ 804.225.1897 ✉ info@ssva.com
804.288.3338 www.ssva.com

Strategic Solutions
OF VIRGINIA