Mobile Banking App is HERE!

UNION BANK

JANUARY 2020 Issue 1

Why Traditional Security Controls May Not Be Enough

Member FDIC

EQUAL HOUSING LENDER

Years ago, being able to spot an internet scam was very clear cut. Even when threats became more complex, they could easily be identified using policy, signature, and black list based defenses. But the speed of advance technology has allowed cyber criminals to refine their techniques which makes it much more difficult to detect.

We know these new techniques from cyber criminals have been working because even well known applications and websites including banks, retailers, and large corporations have been compromised. We no longer can determine who the enemy is or from where they might launch their next attack. Cybercriminals are now sophisticated entities who have built a business on stealing and committing fraud against innocent victims.

Cybercriminals have figured out savvy ways to infiltrate networks and sometimes go undetected for months while they lurk in the background stealing sensitive and private information. They have managed to bypass some of the traditional controls that many thought were bulletproof. Below are some examples of how bad actors are being able to evade being discovered by traditional means of protection.

Bypassing User Account Authentication Systems Using Stolen Account Credentials
Account takeover fraud occurs when a cybercriminal obtains and uses a victim's account authentication details to take control of existing bank or credit card accounts and carry out unauthorized transactions. Over the years the total number of account takeover attempts reported by financial institutions has tripled since 2009.

Cybercriminals have refined their techniques of discovering and exploiting network and application layer based vulnerabilities, using techniques such as SQL injection, through which they steal consumers' usernames, passwords, and private information. Using the stolen credentials, cybercriminals hijack email, social media, banking, and other financial accounts. They are then able to launch attacks anonymously through zombie computers from behind proxy networks. Because the access attempts use the correct username and password, include other valid account details that make the request seem legitimate, organizations are challenged in their ability to ensure the true party is accessing the account.

Continued on page 2

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

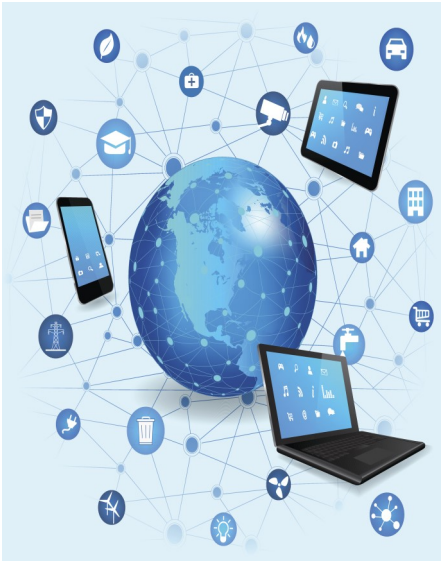
Bypassing Device Identification Anti-Fraud Technologies Using Mitb Malware Attacks

The banking industry often employs two step security measures as an added layer of protection against password theft and fraud. But several new Man in the Browser (Mitb) style attacks have recently been shown to be able to defeat even two-factor authentication systems.

Mitb is an internet threat that takes advantage of the vulnerabilities in a web browser which allows a cybercriminal to change content or even add on transactions etc. Using the Mitb method, a cybercriminal constructs a fake bank website and entices the user to that website. The user then inputs their credentials and the cybercriminal in turn uses the credentials to access the bank's real website. When executed well, the victim never realizes they are not actually at the legitimate bank's website. The cybercriminal then has the option to either abruptly disconnect the victim and initiate fraudulent transactions themselves, or pass along the victim's banking transactions to minimize suspicion while making their own transactions in the background.

Bypassing Ecommerce Fraud Detection Systems Using Tor and Proxy Hidden Attacks

For most organizations their website is the primary channel for communicating and handling transactions with customers, potential customers, partners, suppliers and even employees. Consequently, it is also one of the primary attack paths used by cybercriminals when targeting an organization for ecommerce fraud as well as security compromise and breach.



Ecommerce over the past decade has become the main way for many to conduct everyday shopping needs, from purchasing an assortment of products to even purchasing groceries. There is absolutely nothing you can't buy online. Fraudsters have also moved with the times and evolved their efforts by increasing automation and creating botnets. Botnets is a network of private computers infected with malicious software and controlled as a group without the end user having any knowledge. But over time those botnets transitioned into malnets. Malnets are extensive malware networks circulating the internet and are capable of producing mass market attacks on a constant basis. Malnets pose an increasing threat on the ecommerce landscape.

Botnets and Malnets are not the only method, there has also been an increasing use of Tor. Tor is short for the "The Onion Router" which essentially is a the ability for users to browse the internet anonymously. It was originally used by the US Navy but was made available to the public. These types of services have created a new security and fraud challenge for businesses and organizations that conduct business and process transactions online. Fraudsters use this as leverage and are able to rapidly change locations to avoid being traced and initiate transactions from locations that seem to be legitimate or may even be the cardholder's actual compromised computer.

These are just a few examples of how cybercriminals can circumvent some of the most protected networks. It serves as a reminder that everyone must remain vigilant. Many have made it their mission to create products that help protect companies and everyday people from these types of attacks. They recognize that if the landscape of traditional cyber attacks is changing, so must the approach and response to fight against it.

Sources:
https://www.investopedia.com/terms/t/tor.asp
https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
https://nakedsecurity.sophos.com/2019/10/11/hackers-bypassing-some-types-of-2fa-security-fbi-warns/

What to Expect in 2020

Happy New Year! We are all excited to enter into a new decade. But like every year before it, 2020 will be faced with expected and unexpected security challenges.

Big questions that we all wish we had the answers to still remain, such as, what will be the biggest security threats? What solutions will be most beneficial? Of course, no one has a crystal ball, but many experts are making their predictions. TrendMicro in particular has wrote extensively about what they believe 2020 will hold for the cyber world. It's clear that things will become more complicated and protecting networks will remain a top priority.

Trend Micro has done an in depth look at the platforms, applications and services that will require protection. Their predictions are based on their expert opinions and knowledge of technologies and the emerging threats. In their November write up titled "The New Norm: Trend Micro Security Predictions for 2020" they go into great detail about the what and the how of cyber security threats.

Below are a few of the important predictions on their list:

- *Banking systems will be at risk with open banking and ATM Malware.*
- *Cybercriminals will outpace incomplete patches.*
- *Deepfakes—fake audio or video recordings that look and sound like the real thing will become more prominent.*
- *Bad actors will capitalize on the IoT devices for extortion.*
- *Cloud platforms will be subject to code injection attacks.*

No one can tell the future, but what we do know is the cyber world is complex and ever changing. We also know with appropriate planning, education and protection an organization can mitigate many of these threats. So, let's hope for the best and welcome 2020 with open arms!

"It's clear that things will become more complicated and protecting networks will remain a top priority."

Sources:
https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2020