# Barbarians at the Gate: Current Threats and Attack Types

accume partners

In the past 18 months, Accume Partners has responded to and investigated scores of security incidents involving a variety of attack techniques. According to Symantec, last year malware variants were up 88%, representing almost 661 **billion** unique malware variations. Based on numerical evidence alone, it's clear that businesses are under significant attack on all fronts. In this paper I will provide an overview of some of the successful attacks that Accume Partners has witnessed and explain some simple steps that you can take so that your institution doesn't become another statistic.

Bob Gaines, Director

646.375.9500 x114

rgaines@accumepartners.com

## Fileless Malware

Fileless malware is becoming the leading threat vector for attacks. According to Ponemon, 76 percent of successful attacks in 2017 leveraged this type of malware, making it four times more likely to succeed in compromise compared to traditional attack techniques. Unlike other forms of malware, fileless malware attacks don't install software on a victim's machine. Instead, it runs all of its functions in the computer's memory (RAM) so that it can avoid most forms of detection. In addition, it often leverages tools that are built-in to Windows to carry out attacks, using Windows against itself as another form of evasion. Once the infected machine is rebooted, the malware and all of its artifacts are also deleted, making detection and investigation after the fact very difficult.

**Sample Attack**

**Step 1:** A phishing email convinces a user to click on a link and visit a website.

**Step 2:** The website has a malicious variation of flash on it. When it loads on the local system, it delivers the payload.

**Step 3:** Flash accesses PowerShell and only runs in the computer's memory: instructions go through the command line, unseen by the user. Those instructions tell it to download a malicious PowerShell script specializing in collecting sensitive data and sending it back to its creator.

What you can do to prevent this type of attack

- Disable PowerShell and WMI if you're not using them.
- Disable macros if you're not using them. If you are, digitally sign and use only those vetted specifically for the company. No signature means don't use it!
- Regularly check security logs for large outbound data sets leaving the network.

- Ensure that firewalls, web filters and IDS/IPS are dynamically updated to keep their protections current
- Keep operating systems and applications patched

## Malvertising and Watering-Hole Attacks

A recent Symantec report determined that 1 in 13 URLs analyzed at the gateway were found to be malicious. These malicious sites are often the locations for Malvertising and Watering-Hole attacks. A **watering-hole attack** is a targeted social engineering strategy that capitalizes on the trust users have in websites they regularly visit. The victim feels safe to do things they would not do in a different situation, such as downloading applications or responding to popup messages. **Malvertising** (a blend of "malicious advertising") is the use of online advertising to spread malware. Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages. These attacks function in a similar way, but deliver different payloads. During investigations only a detailed analysis of the user's web history can accurately determine one attack from another, but both represent a failure in one or more security controls.

In one high-profile attack, the New York Times, the BBC, AOL and NFL were tricked into running malicious ads that hijacked computers, encrypted user data and demanded ransom payments for recovery keys. Combined, the targeted web sites had visitor traffic in the billions.

**Sample Attack**

**Step 1:** A user browses to a website as a function of their normal habits

**Step 2 (Watering Hole Attack):** The user downloads a file or clicks a link within the page that they assume is a normal function (a report or an update). What they download has a malicious payload (i.e. Trojan)

**Step 2 (Malvertising)**: Once the malicious ad loads in the user's browser (which is an automatic function) it immediately launches an attack on the browser or the operating system, typically exploiting an unpatched vulnerability. The attack runs in memory, without the user seeing anything.

**Step 3:** The malicious payloads run in the background on the user's machine until it is detected.

What you can do to prevent this type of attack

- Leverage web filters to block sites that don't have a legitimate business purpose
- Disable PowerShell and WMI if you're not using them.
- Regularly check security logs for large outbound data sets leaving the network.
- Ensure that firewalls, web filters and IDS/IPS are dynamically updated keep their protections current
- Investigate in "hardening" applications and operating systems using secure configurations standards (i.e. "STIGS")
- Keep operating systems and applications patched

## Email Account Takeover

An Email Account Takeover (ATO) is obtaining a legitimate user's details to take over their online accounts. The attacker then uses this account to launch subsequent email attacks for financial gain or to execute a data breach. The security firm Agari sites a 126% increase month to month in targeted email attacks that exploit Account Takeover tactics since the beginning of 2018. Osterman Research reported that in the last 12 months, 44% of organizations were victims of targeted email attacks launched via a compromised account. ATO-based attacks are particularly dangerous and effective because they originate from email accounts of trusted senders. This has two important ramifications: First, because there is a pre-existing trust relationship with the sender the attack is very likely to succeed. Second, because the attack originates from a legitimate account, they go undetected by traditional security controls.

**Sample Attack**

**Step 1:** Attackers can gain access to a user account by launching a phishing or malware based attack to capture a user's ID and password, or conduct a "credential stuffing attack" using old usernames and passwords.

**Step 2:** Once an account has been accessed the attacker establishes account control by setting up forwarders to silently monitor user communications, change log settings to avoid detection and modify passwords to maintain password control.

**Step 3**: Once account control has been established the attacker will conduct reconnaissance to determine how the compromised account can be exploited, and how far the attacker can traverse the system or network without being detected.

The #1 cause of successful ATO attacks is password reuse.

Over 2.3 Billion usernames and passwords were reported stolen (spilled) from 51 organizations in 2017.

**Step 4**: Depending on the type of information gleaned from reconnaissance the attacker will launch an email attack targeting the contact list of the controlled account. This may involve a Business Email Compromise attack to extract funds or a targeted phishing campaign to other employees aimed at gaining a deeper foothold into the organization.

**Step 5**: Depending on the type of email attack employed, the attacker will exfiltrate the sensitive information or funds, or, if user account credentials were requested, repeat the ATO process.

What you can do to prevent this type of attack

- Use DMARC as an enhancement to your email protections
- Investigate blocking IP blocks from countries your institution does not **do** business with, as many ATO attacks originate overseas.
- Implement multi-factor authentication for email and remote-access solutions.
- Check email logs regularly for unauthorized access attempts, logon attempts from unknown IP addresses and new ruleset creations
- Ensure that firewalls, web filters and IDS/IPS are dynamically updated to keep their protections current

- Keep users informed of social engineering techniques for credential harvesting
- Keep operating systems and applications patched

## Business Email Compromise

A business email compromise (BEC) is an exploit in which the attacker tricks the target or targets into sending money to the attacker's account. According to the FBI's Internet Crime Complaint Center (IC3), "the BEC scam continues to grow, evolve, and target businesses of all sizes. Since January 2015, there has been a 1,300 percent increase in identified exposed losses, now totaling over $3 billion." Although the attackers use a variety of tactics to fool their victims, a common scheme involves the criminal group gaining access to a company's network through a spear-phishing attack and the use of malware. Undetected, they may spend weeks or months studying the organization's vendors, billing systems, and the CEO's style of e-mail communication and even his or her travel schedule. The most common victims of BEC are companies that use wire transfers to send money to international clients.

**Sample Attack**

**Step 1:** Organized crime groups target a business, exploiting information available online to develop a profile on the company and its executives

**Step 2:** Spear Phishing emails and/or telephone calls target victim company officials (typically an individual identified in the finance department.) Perpetrators use persuasion and pressure to manipulate and exploit human nature. This grooming may occur over a few days or weeks.

Note: It is not uncommon for BEC attacks to originate from a successful Account Takeover Attack (ATO).

**Step 3**: The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

**Step 4**: Upon transfer, the fund are steered to a bank account controlled by the organized crime group.

What you can do to prevent this type of attack

- Use DMARC as an enhancement to your email protections
- Configure your email system to add headers to incoming emails from outside the organization to prevent phishing attacks (i.e. Warning – external email; exercise caution.)
- Keep users informed of social engineering techniques for BEC Attacks
- Verify changes in vendor payment location by adding additional dual controls such as having secondary sign-off by company personnel.
- Confirm requests for transfers of funds by using phone verification as part of a two-factor authentication; use previously known numbers, not the numbers provided in the e-mail request.
- Carefully scrutinize all e-mail requests for transfer of funds to determine if the requests are out of the ordinary.

*Don't know where to start? Contact Accume Partners and we will get you on the proper path to a threat intelligence solution that works for you*