GLASSWALL

Threat Intelligence Bulletin

Evasive Spear Phishing

Part 1

August 2019

by Lewis Henderson

Glasswall Threat Intelligence Bulletins mine our Threat Intelligence Platform to explore the latest trends in evasive malware that bypasses the various security layers designed to protect an organization. This first part of a two part special Bulletin is a joint effort between Glasswall and Forcepoint, the Raytheon-owned military provider of world class gateway security solutions. Both organisations share a passion for enabling our customers to defeat and disarm those who intend to harm and disrupt.

The topic of this Bulletin is so new it required us to create a new category of threat—

Evasive Spear Phishing

This threat presents one of the highest business risks in terms of financial and reputational impact, yet represents the lowest occurring threat in terms of volume that an organisation needs to defend against.

Our analysis of over 25m email attachments reveals some alarming statistics about the evasive spear phishing threat.

Key Bulletin Findings

1. Technology is the most targeted sector, followed by Legal and Industrial Control Systems Providers
2. Theft of Intellectual Property and Client Confidential data are highest risks
3. Users are more likely to click or open documents that appear familiar from a known source
4. On average 1 in every 35,000 emails contains highly targeted Spear Phishing
5. 70% of all Evasive Malware events are Spear Phishing alone

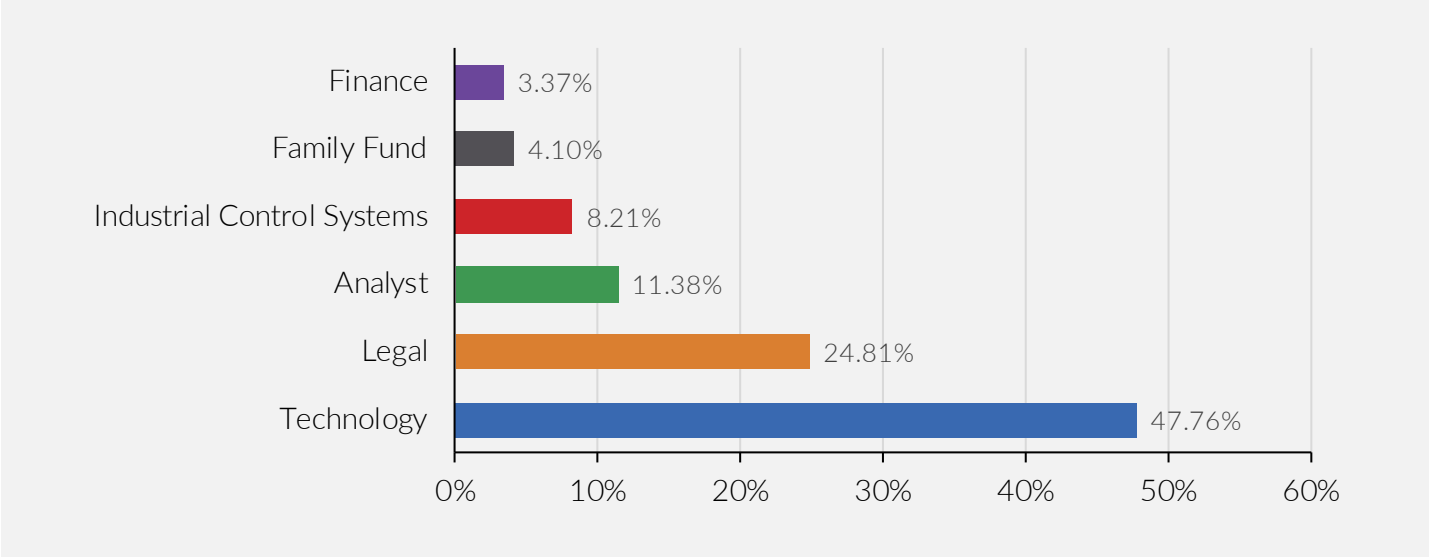
Let's start with the usual definitions, just to be clear. Phishing is a well-known tactic: Spear Phishing takes this to the next level, but falls short of describing totally unique events, one among millions of daily events that occur across the IT infrastructure. Thus we needed to define a new category: Evasive Spear Phishing: A unique malicious file, being sent from one actor to one recipient.

Malicious actors are getting continually better not just at evading legacy technologies, but at tactics for precisely targeting specific individuals and adapting the techniques they use to do so. For the attacker, putting effort into creating an Evasive Spear Phishing attack is clearly a successful method, since it is reported as the cause of 90% of successful hacks and data breaches*. The users who are their targets are more likely to unintentionally start a malicious process as a victim of Spear Phishing simply because the harmful emails and documents they're sent are utterly convincing as legitimate business communications (we'll explore this later in the Bulletin).

Let's explore what we at Glasswall and Forcepoint are seeing in these attacks:

Industry Focus

Slicing our customer data by distinct sectors and highlighting the risks associated with each provides insight as to why malicious actors go to the effort of creating such time consuming, resource intensive techniques and under-the-radar tactics. Their key objective remains the theft of highly valuable or influential information or data that can be monetised, but their targets can vary.



*2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics: Cisco and Cybersecurity Ventures

As shown below, each sector faces different risks to be mitigated, providing rich and unique pickings that also require malicious actors to adapt their approach accordingly:

Technology Manufacturers

Most targeted role: Software Developers
Risk: loss of intellectual property
Impact: loss of revenue

Legal

Most targeted role: M&A Lawyers
Risk: loss of client confidential data
Impact: loss of customer trust and company reputation
[these are higher threats than legal liability]

Global Professional Services (Accounting)

Most targeted role: Corporate Account Managers
Risk: loss of company data
Impact: loss of revenue

Industrial Control Systems

Most targeted role: Admin
Risk: nation state espionage or ransomware
Impact: threat to critical national infrastructure, loss of services and customers

Family Investment Funds

Most targeted role: Family Members
Risk: stolen account details and loss of financial assets
Impact: loss of financial assets via unauthorised transfers

Finance

Most targeted role: Administrators
Risk: loss of customer data or inside trading data
Impact, loss of customer trust and share value

Email Attachment Focus

Now that we're aware who is in the cross hairs for Evasive Spear Phishing, let's turn our attention to the tactics and methods the malicious actors are using.

When it comes to email attachments, there are consistently two primary weapons of choice: .PDF files and older Binary format ('97-'03) Word documents, which we've covered in a previous Bulletin.

What we know about the Evasive Spear Phishing email attachments:

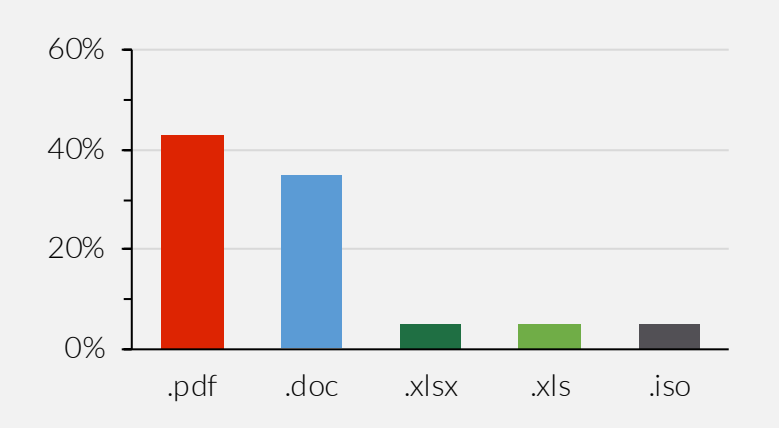
- Attackers are leveraging every day file formats
- 43% were .PDF files, 35% were Microsoft Binary format ('97-'03) Word documents
- Files contained highly specific content related to the company and human targets

If we look across other file attachment types, there is a significant drop off when we encounter the next most used file type: Microsoft Excel files. This indicates that the attackers are taking time to craft convincing .PDF and Word documents with visual markers such as company logos and/or written text referring to invoices or payments so as to obscure the veiled malicious purpose of the email attachment.

Remember that not all of these files actually do anything immediately obvious or suspicious to the user (we'll explore further down), ensuring that the attack is both evasive and silent.

.PDF and Word documents favoured by attackers for Spear Phishing Attacks

Excel files were significantly lower, followed by .iso which is an image of a CD/DVD



File Content Focus

We're building a profile that shows highly risk-averse organisations are the ones getting targeted by Evasive Spear Phishing, and we can see attackers are typically using day-to-day file formats such as .PDF and Word – but what in those files is the indicator of compromise?

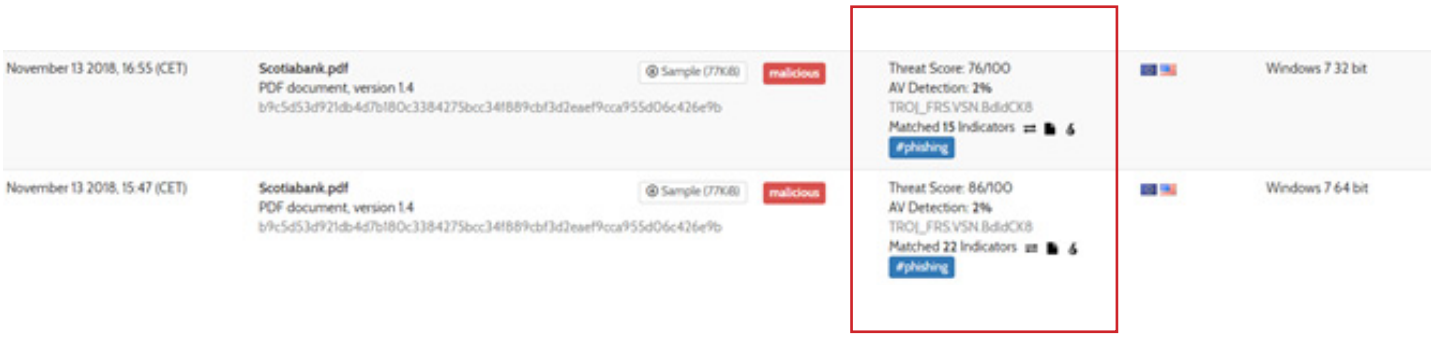
If we split them into file types, the picture becomes clear how attackers are leveraging both weaknesses and exploits in the files themselves, in addition to 'hiding in plain sight' behind standard features that users interact with on a daily basis.

.PDF Spear Phishing Insights

Unsurprisingly, Glasswall sanitised URL links from around 95% of .PDF files classified as Spear Phishing—it's the oldest Phishing trick in the book to attempt to get a user to click and discreetly open a browser session that downloads files—but here's what was interesting about these files:

- On average, only 3 out of 60 Anti-virus (AV) vendors classified them as malicious after 6+ months
- The malicious websites that host the malware are temporary, to hide an attacker's identity
- Scams like VOIP voicemail and fake invoices feature to lure users into clicking links

The example below processed through Hybrid Analysis shows the first seen date as November 2018, yet by July 2019 there was only a 2% AV detection rate:



Word Spear Phishing Insights

The same feature appears again and again within Malicious Word files: Macros.

Macros are used in 93% of Spear Phishing attacks that use the older Binary Word formats designed for the Windows XP era. The question really has to be how much longer can organisations continue to justify allowing in these formats whilst they pose one of the greatest risks?

Here are some other findings that relate to this highest threat Glasswall has seen so far in 2019:

- 93% contain a Macro, and only 6% contained additional embedded files
- Only 1% contained URL links that directed the user towards a malicious website

Excel Spear Phishing Insights

Some examples of malicious Excel files contained clear indications of advanced techniques such as File-less Malware (explored in a previous Bulletin), which is the absence of an actual malware payload as part of the initial delivery. Here we saw samples that used a combination of Dynamic Data Exchange (DDE) and Embedded Files working in tandem to kick off a malicious process that simply bypasses technologies looking for known bad or suspicious file behaviour.

Part 1 Conclusions

Attackers are fully wising up to the reality that 'spray and pray' techniques that used to work now need much more effort upfront. A significant part of their overall strategy must involve intelligence-gathering and reconnaissance, so their method of Evasive Spear Phishing can be delivered with surgical precision. Although this article shines a light on unique incidents among millions, these sometimes add up to a bigger picture. Consider these two true examples:

Customer: Critical National Infrastructure

A supply chain partner was breached, and two unique .PDF files were targeted at employees in the Finance department. The attacker's objective of deploying ransomware failed, but the attack highlights that lowering your guard with supply chain partners is not an option.

Customer: Global M&A Law Firm

A Senior Partner was targeted by a single threat actor over the course of two days, with 11 Word documents and no less than 6 unique malware variants. After the series of attempts failed, the attacker's final sign-off was a file containing ransomware to be triggered by a Macro; fortunately Glasswall sanitised it. The Senior Partner shrugged it off as suspicious and reported it to Support.

Part 2 Preview

In the upcoming second Bulletin on Evasive Spear Phishing, our co-author Forcepoint will deep dive into some of the malicious files we encountered as part of our research, and reveal the attacker techniques and tactics in greater detail.

About Glasswall

Glasswall Solutions has offices in the United Kingdom and across the United States, and provides organizations and government agencies with unique protection against evasive, sophisticated cyber threats in files and documents through its innovative, ground-breaking security d-FIRST™ technology.

GLASSWALL

Head Office

+44 (0) 203 814 3890
info@glasswallsolutions.com
Continental House, Oakridge,
West End, Surrey, GU24 9PJ

Sales

UK: +44 (0) 203 814 3890
USA: +1 (866) 823 6652
sales@glasswallsolutions.com
us.sales@glasswallsolutions.com

Technical Support

support.glasswallsolutions.com
(Registered Users only)

Investors

+44 (0) 203 814 3890
investorrelations@glasswallsolutions.com

Press & Media

Whiteoaks International: +44 (0) 1252 727313
W2 Communications: +1 (703) 218-3555