Discussion Paper

mimecast threatintelligence

We're delighted to include this first newsletter copy from one of our Platinum sponsors. Mimecast's article on cyber criminals and the risks faced by voluntary sector organisations:

Charity sector

The charity sector is a highly attractive target for cyber Threat Actors due to the amount of money they handle, the sensitive information they handle and store (including personal, financial and commercially sensitive data), and often the lack of funding and knowledge surrounding cyber security.

The sector faces many of the same threats that we see across other industries, and remains highly vulnerable due to charity/non-profit company structures, the lack of funding for cyber security and being attractive targets for data harvesting and targeting large donations.

Why is the charity sector targeted?

The charity sector is an attractive target for cyber criminals and Threat Actors seeking a soft target to extort money and sensitive information from. Charities hold funds, receive donations, and handle personal and commercial information that is of monetary value to cyber Threat Actors. In many cases they also conduct activities internationally (for example aid charities), gathering information and evidence of issues such as war crimes, breaches in international law and other such atrocities that make their e-mails and computer systems a prime target for stealing information that could potentially be damaging for foreign governments and organisations.

There is considerable evidence from open source reporting that cyber security awareness across different charities, and their approaches to security, vary considerably. This leaves the sector vulnerable, as many Threat Actors know that many charities are less likely to be investing in cyber security practices, but often cash rich with donations and data. It is likely they are seen to be easy targets to extort with ransomware, with evidence from open source reporting suggesting many charities are keen to keep cyber attacks quiet for fear of reputational damage and the chance of missing out on donations.

Research conducted by the UK government[1] revealed there are also concerns with impersonation attacks (but not necessarily e-mails – there is activity whereby Threat Actors will take over the charity website, or impersonate one, highly likely in the effort to re-direct donations being made and re-direct legitimate activity to gain valuable data and information).

What are the effects of cyber-attacks on the charity sector?

Cyber-attacks are estimated to cost charities anything from hundreds of pounds, right through to over £100,000. This level of cost from cyber-attacks could be potentially devastating.

However, due to a lack of funding and knowledge about how to tackle cyber threats, it is likely that many charities are either unaware they have been targeted, do not see themselves as a

[1] National Cyber Security Centre – Cyber Threat Assessment: UK Charity Sector, Febrruary 2018.

target or will not report cyber-attacks out of fear of reputational damage and the possibility of missing out on funds in the future.

What targets the charity sector?

Sophisticated Impersonation Attacks

Social engineering (most commonly through impersonation) remains a top tactic for threat actors. Mimecast witnesses this activity constantly evolve to deceive end users, with a large increase in these types of attack identified throughout 2019. This leads to further activity, including impersonating domains, subdomains, landing pages, websites, mobile apps, and social media profiles. All of these are used, many times in combination, to trick the target organisation and/or its employees into surrendering credentials and other personal information or installing malware.

Individuals at the senior and C-suite level are frequently impersonated, with Threat Actors targeting those they believe are closely associated with the impersonated individual, such as a personal assistant. These relationships are often easily discoverable using social media platforms,[2] and this information makes it easy to identify reporting hierarchies within an organization. Analysis of a selection of these emails found that they are successfully employing relatively unsophisticated methodologies, such as coercing the victim into doing something they shouldn't using social engineered content within the main body of the email, instead of including malicious URLs or attachments.

Insider Threats

Most organisations are heavily focused on protecting their organisations from inbound attacks, often via e-mail. However, not enough emphasis is being put on protecting against threats that originate from the inside the company itself.

Mimecast's recent *The State of Email Security for 2019* report investigated the main email security challenges facing organisations today, including the internal threat issue. What they found, via a global survey of IT and security leaders, was:

- 41% of organisations have seen increases in internally-sourced threats/data leaks, year-over-year.
- 71% of organisations reported having seen attacks where malicious activity was spread from one infected user to another. This was up from the previous years' report.
- 86% of respondents reported that their organisation had experienced threats/data leaks caused by careless employees.
- 95% of security breaches are directly contributed to by human error.

Ransomware

[2] https://mashable.com/article/linkedin-is-full-of-spies/

When ransomware infects computers, it will encrypt files and folders on the victim's operating system, sometimes partitioning parts of the harddrive, and preventing access and often halting all commercial operations if it spreads through the network.

The aim of ransomware is to extort the victim for money, often with demands to deposit money in cyrptocurreny wallets, in exchange for the decryption key. However, not all threat actors follow through with their promise once the money has been paid, with victims then out of pocket and still having no access to their files and folders.

Most ransomware infections start with:

- Email messages with attachments that try to install ransomware.
- Websites hosting exploit kits that attempt to use vulnerabilities in web browsers and other software to install ransomware.

Ransomware-as-a-service has increased in popularity too, with threat actors developing and establishing a solid business model of creating the malware and selling it on the dark web (and sometimes brazenly across the open internet too on occasion) to other cyber criminals and threat actors. The buyers then operate the ransomware and split the profits along a pre-defined agreement with the creators.

Phishing

Sending phishing e-mails is one of the most common cyber Threat Actor activities and successful infection vectors. Phishing e-mails are the most affordable infection vector in terms of investment and the level of expertise required to be successful, making them highly attractive to amateur Threat Actors.

Successful phishing campaigns can result in profits almost immediately, allowing a Threat Actor to cash out as soon as possible or sell the data/PII information on to criminals or other Threat Actors for a good price on the black market. The charity/non-profit sector is an attractive target for this very reason.

Often Threat Actors will conduct reconnaissance on their victim in order to send them a spear phishing e-mail. The Threat Actor will identify a vulnerable banking infrastructure and then look on platforms such as social media to identify individuals who work there, much the same as their methods for impersonation e-mail attacks. The e-mails they then send out is a very convincing spear-phishing e-mail and trick the victim into giving them access to the banking infrastructure/networks they are trying to target.

Observed attacks on the charity/non-profit sector – Mimecast threat landscape

Within the Mimecast threat landscape, from 1st February 2019 to 31st July 2019, 2.97 million threats were blocked across the following categories:

Spam

Spam is used to target a large number of industries and customers at the same time, often using e-mails that have been scraped from data breaches and exposed company e-mails on the open web. Spam e-mails are used to spread threats, with these campaigns highly likely to be part of more dangerous cyber-attacks, where large botnets are used to distribute high numbers of e-mails to increase the effectiveness of the cyber-attacks.

One of the most prolific spam campaigns currently hitting the landscape is from the ever-evolving threat of Emotet, which uses its spam module to spread the Emotet botnet (highly likely to be a number of botnets acting together). The spam module spreads emails via the botnet which contain malicious URLs within the main body of the e-mail, or malicious attachments that lead to victim into unknowingly downloading Emotet.

Impersonation Attacks

Impersonation e-mail attacks remain a consistent, unsophisticated, approach to targeting individuals within companies.

Mimecast analysis of the impersonation e-mails indicates targets for the impersonation itself remain among the senior and c-suite level, with Threat Actors gravitating towards targeting those they believe are most closely associated with the impersonated individual (i.e a personal assistant). It is likely they gain this information via social media platforms such as LinkedIn, often a strong source of information linking company alumni together, along with the departments the targets work within; often making it easy to connect who works for whom within an organisation.

Mimecast has analysed submissions of these e-mails during 2019, indicating methods of un-sophisticated attacks (e-mails which do not contain malicious URLs or attachments, instead coercing the victim into falling for the social engineering strategies within the main body of the text) continue to be successful and Threat Actors are finding different techniques to successfully land these fraudulent e-mails into victim's inboxes.

Known Malware

Mimecast has blocked a large amount of 'Known Malware' threats to the charity/non-profit sector over the period 1st February 2019 to 31st July 2019. Known malware are threats that Mimecast have identified and categorised, continuining to block updates to these threats. This category includes trojans, downloaders, exploits, droppers, phishing, javascript malware, html attacks, worms, ransomware and viruses.

Research throughout 2019 has indicated an increase in a trend that has been growing over the last few years and is demonstrated across the data displayed in our blocked 'Known Malware Attacks'; that cyber-attack campaigns are becoming increasingly complex because they are often not just one attack anymore.

As the security industry becomes increasingly talented at blocking new threats, it is highly likely Threat Actors will start to create malware that is highly complex, with multiple layers of complex obfuscation, in order to trick and circumvent AV scanners.

Advanced Malware

Discussion Paper

Over the reporting period April – June 2019, Mimecast has blocked a large amount of Advanced Malware threats. Advanced Malware are new attacks attempting to target our customers but are previously not known to AV scanners, and therefore not categorised yet. *Mimecast blocked all of the advanced attacks displayed in Figure 1 below.*

Discussion Paper

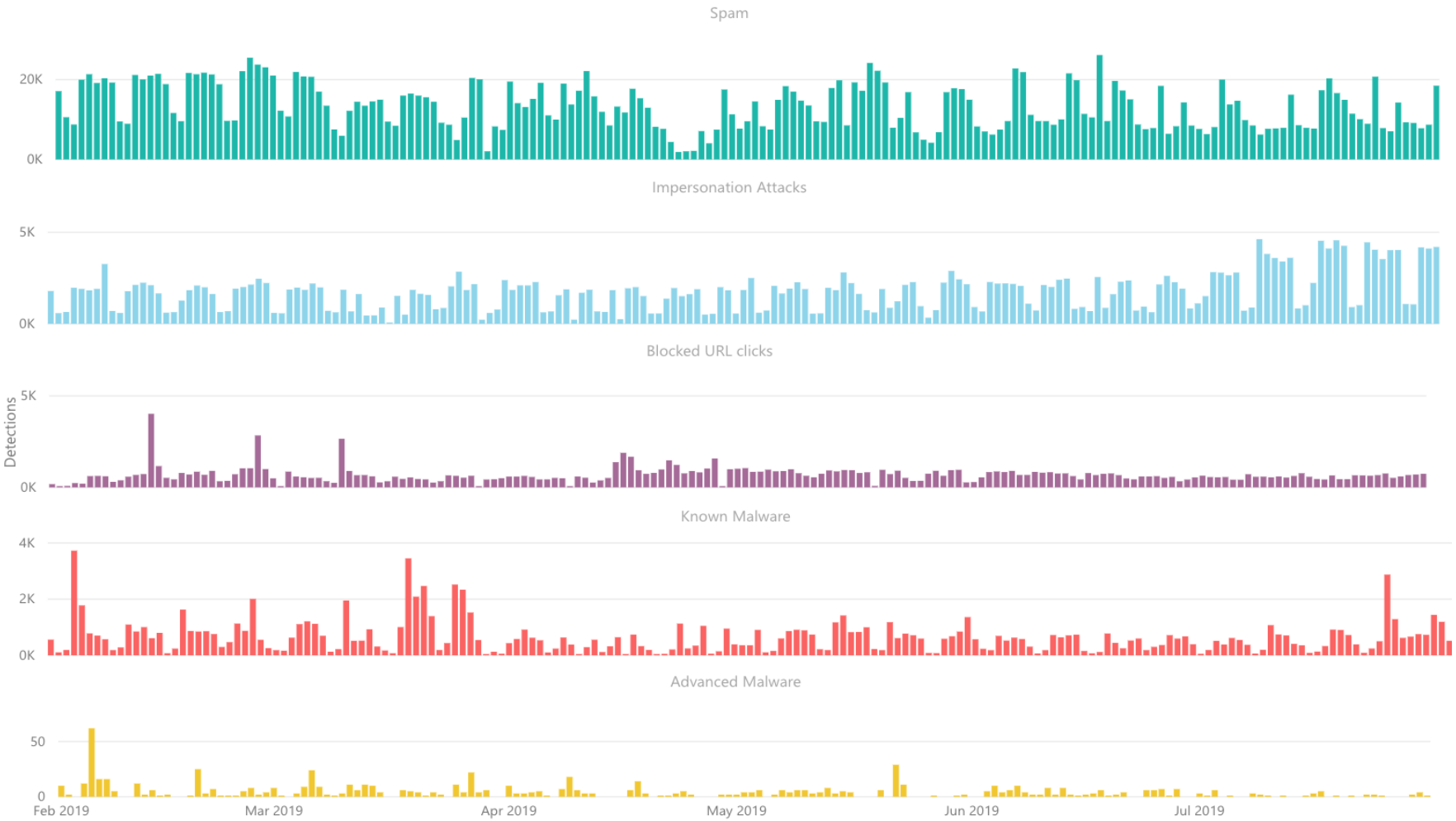

Figure 1: Blocked Threats for the charity/non-profit sector (1st February 2019 to 31st July 2019)

Is the threat going to go away?

Simply put, no, the threat is enduring to this sector, as with all business areas. Threats are not always directed at the charity/non-profit sector and it is highly likely they are suffering breaches and other cyber attacks by outsourcing key IT operations and the security of their data to third party support companies[3].

Along with a range of differing levels of security awareness in this sector, there are larger concerns by government researchers and the NCSC that not enough money is going into cyber security efforts for this sector.

Malicious insider threats are likely to pose an ongoing threat to chairities, with fraud and corruption large concerns within this sector. This type of activity can include an employee who passes on credentials to cyber Threat Actors in exchange for financial gain, or conducting activities such as stealing data for other nefarious purposes.

Negligent insider threats include carelessness from employees and breaches of security procedures resulting in cyber attacks being allowed to happen (i.e opening a malicious attachment).

The charities/non-profit sector often operate internationally, in conflict zones, and delivering aid and other such items into difficult and dangerous areas of the world. Often charities operating in these difficult conditions are useful sources of information for governments and other agencies to understand the dynamics of conflicts and wars and as such, often gather evidence of humanitarian crimes, making them quite powerful in their influence on domestic and foreign policy. It is highly likelty this makes them potential targets of nation state attacks, who are likely to be looking to erase evidence of crimes, destroy the organidsations reputations or completely wipe them out financially so they are no longer able to operate and gather information/evidence.

[3] NCSC – Cyber Threat Assessment: UK Charity Sector, February 2018.