REPORT

proofpoint.

AN OUNCE OF PREVENTION

A 12-MONTH ANALYSIS OF RANSOMWARE, EMAIL FRAUD AND OTHER HEALTHCARE THREATS—AND HOW YOU CAN STOP THEM

proofpoint.com

TABLE OF CONTENTS

INTRODUCTION

Healthcare is under siege. Cyber attacks are exposing personal data. Ransomware is shutting down emergency rooms. Fraudulent emails are defrauding partners, patients, and your own staff.

To help healthcare organizations better understand this changing threat landscape, we analyzed a year's worth of cyber attacks against care providers, hospitals, and insurers.

If you're in healthcare, work with healthcare companies, or trust your most personal data to those in the industry, this threat report is for you.

You'll see how attackers are exploiting human nature to steal money, data, and more. You'll understand the techniques they use to hijack trust—healthcare's most valuable currency. And you'll learn how to protect your organization from today's people-centered attacks.

IF YOU'RE IN HEALTHCARE, WORK WITH HEALTHCARE COMPANIES, OR TRUST YOUR MOST PERSONAL DATA TO THOSE IN THE INDUSTRY, **THIS THREAT REPORT IS FOR YOU.**

WHY THIS REPORT IS DIFFERENT

Every day, Proofpoint analyzes more than 5 billion email messages, hundreds of millions of social media posts, and more than 150 million malware samples. That gives us a unique vantage point to see and reveal and analyze the tactics, tools, and targets of today's attackers.

Unlike most threat reports, we focused on how attacks targeted people. That's because cybersecurity no longer about finding viruses, worms, and malware. It's not about patching system vulnerabilities, hardening the perimeter, or managing endpoints It's not even about complying with the latest security guidelines.

Cybersecurity, like healthcare, is about people.

METHODOLOGY

This report aggregates data collected from attempted attacks captured by Proofpoint deployments around the world. We examined more than 100 million ransomware emails sent to hospitals, clinics and health insurers in the 12-month period ending March 31, 2018.

All of the examples, details, and screenshots we cite in this report are from real-world attacks. In some cases, we omit identifying details to protect the privacy of the targeted organizations.

KEY FINDINGS

As we analyzed hundreds of millions of malicious emails, one trend stood out: today's attacks target people, not just infrastructure. They trick healthcare workers into opening an unsafe attachment or opening a questionable link that leads to ransomware. They impersonate members of your executive team, instructing staff to wire money or send sensitive information. And they hijack patients' trust with scams that cash in on your organization's brand equity.

Here are our key findings.

RANSOMWARE AND OTHER MALWARE

- Ransomware exploded between Q2 and Q4 of 2017, dwarfing all other types of cyber attacks against healthcare companies combined.
- Locky, the leading ransomware strain, was the top malware overall by a wide margin.
- After peaking in Q3, ransomware traffic collapsed as attackers switched tactics.

EMAIL FRAUD

- Nearly 1 in 5 emails purporting to be from a healthcare organization was fraudulent. About 8% spoofed the email domain of a healthcare organization, a technique you can prevent completely by deploying email authentication such as DMARC (Domain-based Message Authentication, Reporting and Conformance).
- Swapping characters was the most common way to create lookalike domains. Switching "I" and "L," "O" and "0," and "U" and "V," are popular techniques. These characters can be hard to tell apart depending on how they are capitalized.
- More than three out of every four attempts at email fraud used one of these subject lines: "payment," "request," "urgent," or "FYI."

RANSOMWARE
This type of malware locks away victims' data by encrypting it, then demands a "ransom" to unlock it with a decryption key.

EMAIL FRAUD
In email fraud attacks, an email or series of emails purporting to come from a top executive or partner firm asks the recipient to wire money or send sensitive information. It does not use malicious attachments or URLs, so it can be hard to detect and stop.

HOW HEALTHCARE IS GETTING ATTACKED

Most email threats fall into one of two categories: malware-based threats (including **RANSOMWARE**) and non-malware threats.

Malware is code that exploits technical vulnerabilities in the victim's computer system or device. It is usually sent as a file attachment or link within emails that trick the victim into opening or clicking it.

Non-malware threats such as **EMAIL FRAUD** use social engineering to persuade the victim to do something—wire money, send sensitive information, provide login credentials, and more.

Both malware and non-malware threats work because prey on people and the way they work. No matter how well you're managing your IT infrastructure, you can't patch your way out of these people-centered attacks. Human nature is the vulnerability.

RANSOMWARE EXPLODES, THEN ATTACKERS SHIFT TACTICS

Ransomware was the biggest threat by far during the period of this study, extending a trend we first saw in 2016.

As shown in Figure 1, ransomware attacks peaked in Q3. We detected a combined 40 million attacks using malicious URLs or attachments in that quarter alone. That's up from 35 million ransomware payloads in Q2.

Ransomware traffic dropped steadily downward through the fourth quarter before collapsing altogether in 2018 as attackers switched tactics.

We saw a similar ransomware lull in 2016. Given that this attack has proven so lucrative in the past, we've not likely seen the last of ransomware as a threat.

NO MATTER HOW WELL YOU'RE MANAGING YOUR IT INFRASTRUCTURE, **YOU CAN'T PATCH YOUR WAY OUT OF THESE PEOPLE-CENTERED ATTACKS.** HUMAN NATURE IS THE VULNERABILITY.

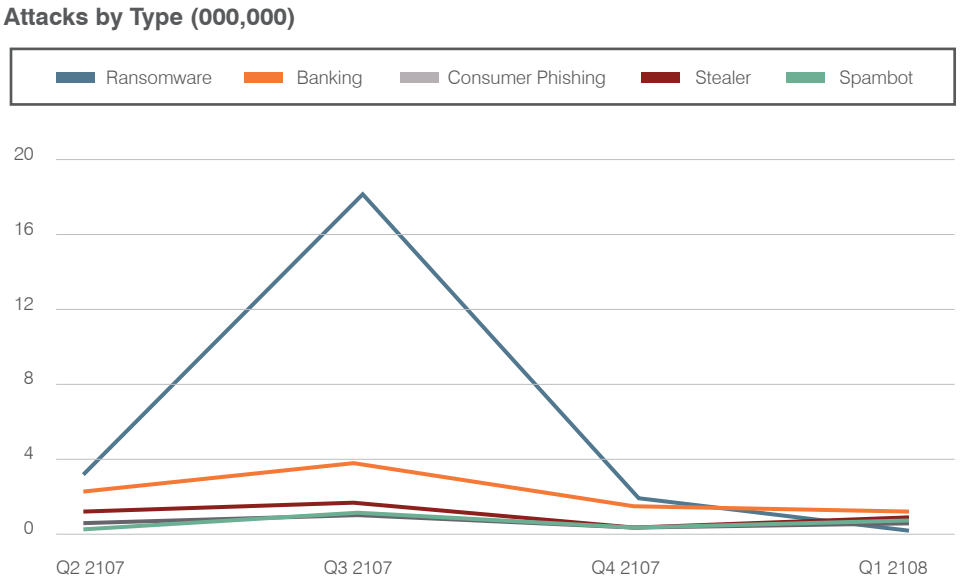


Figure 1: Attacks by type

PHILADELPHIA AND DEFRAY: A TALE OF TWO RANSOMWARE STRAINS

Among the numerous ransomware attacks observed during our study, we saw two especially advanced variants: Philadelphia and Defray. Both strains use customized lures and appeared to target healthcare companies exclusively.

If ransomware makes a comeback in healthcare attacks, we may see more custom variations of the strains we saw in 2017.

PHILADELPHIA

Philadelphia is simple to customize and deploy, lowering the "barriers to entry" for novice ransomware attackers.

In one campaign, attackers targeted clinical staff in selected healthcare institutions (among other organizations in the same city). Email purporting to be from an employee at a targeted company used subjects such as "Patient Referral" and links leading to a download of Philadelphia. The emails used bit.do, a legitimate link-shortening service, likely to evade URL blacklists.

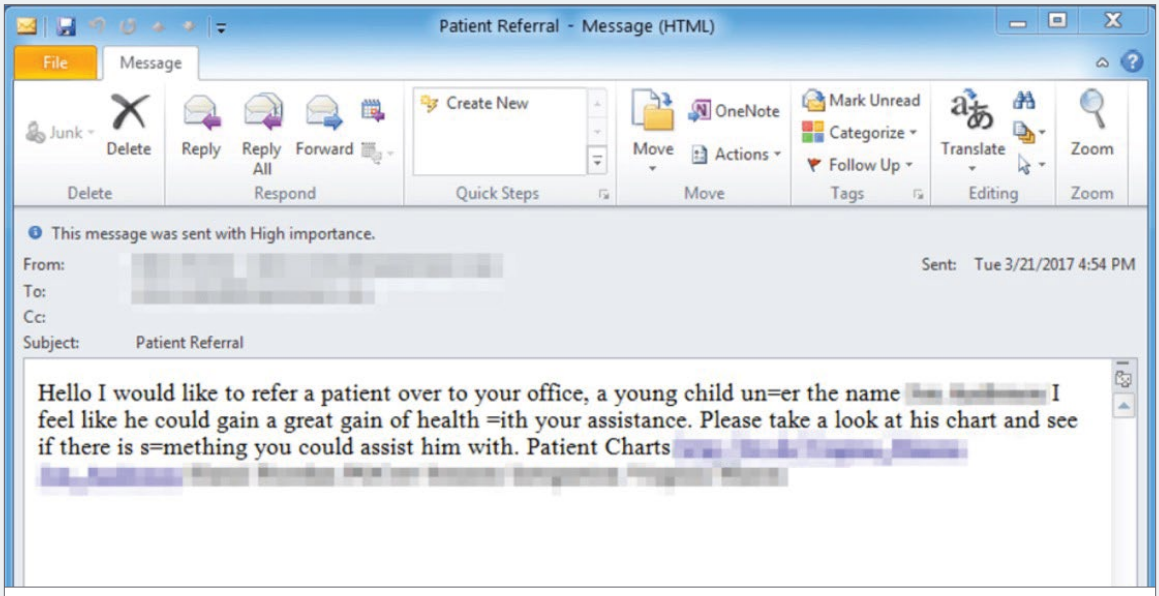


Figure 2: Email sample that dangles the prospect of a patient referral to get the recipient to click.

Figure 2 shows a typical email used in Philadelphia attacks. (We've obscured the header information protect the privacy of the healthcare organization targeted in this attack.) It spoofs the domain name to make it look like it's coming from someone in the same company. This technique is common in targeted emails.

As seen in Figure 3, the attacker customized the ransom demand by:

- Calling out the hospital by name (we've obscured the name to protect the victim)
- Setting the ransom to a high amount of 15 bitcoins (about $18,000)
- Threatening to delete 99 files every 45 minutes

DEFRAY

Figure 3: Custom ransom note sample mentioning the target hospital by name

Defray ransomware has been used in two small and selective attacks, one which was aimed mostly at the healthcare. It gets its name from the command and control (C&C) server hostname from the first observed attack:

defrayable-listings[.]000webhostapp[.]com

Defray attacks have several notable characteristics:

- They spread through Microsoft Word document attachments in email
- The campaigns are as small and targeted
- The lures are custom crafted to appeal to their recipients
- The recipients are people or distribution lists, such as group@ and websupport@
- The emails target recipients U.K. and U.S.

In late 2017, we detected an email campaign targeted at a U.K. hospital. The emails contained a Microsoft Word document containing embedded code (shown in Figure 4). The exploit uses the hospital logo (which we've obscured), and purports to be from the hospital's director of information management and technology.

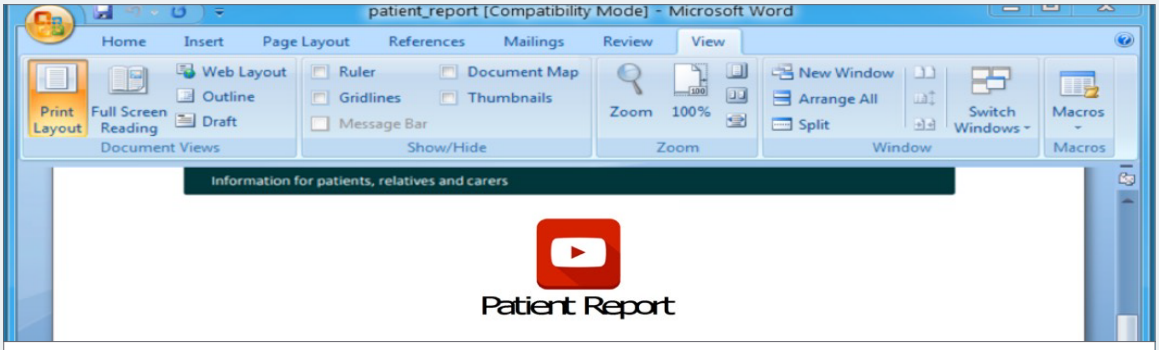


Figure 4: Email used in a Defray ransomware attack

Defray is unusual for ransomware. Unlike most strains, which spread in large, indiscriminate "spray and pray" campaigns, Defray has appeared only in small, targeted attacks. (We are seeing more targeted ransomware campaigns, but they're still rare.)

And unlike many ransomware strains, Defray is not offered for sale as a service or licensed application. Instead, Defray may have been created for the personal of use the attackers using it. We'll likely see it continue to appear in small, targeted attacks.

OTHER MALWARE

LOCKY
Locky uses social engineering to trick users to download the ransomware, which locks and encrypts a large number of systems and file types.

LOCKY was the top ransomware variant and, not surprisingly, the most popular strain of malware overall. But ransomware isn't the only malware threat to healthcare.

As shown in Figure 5, several other malware families targeted health institutions over the course of our study.

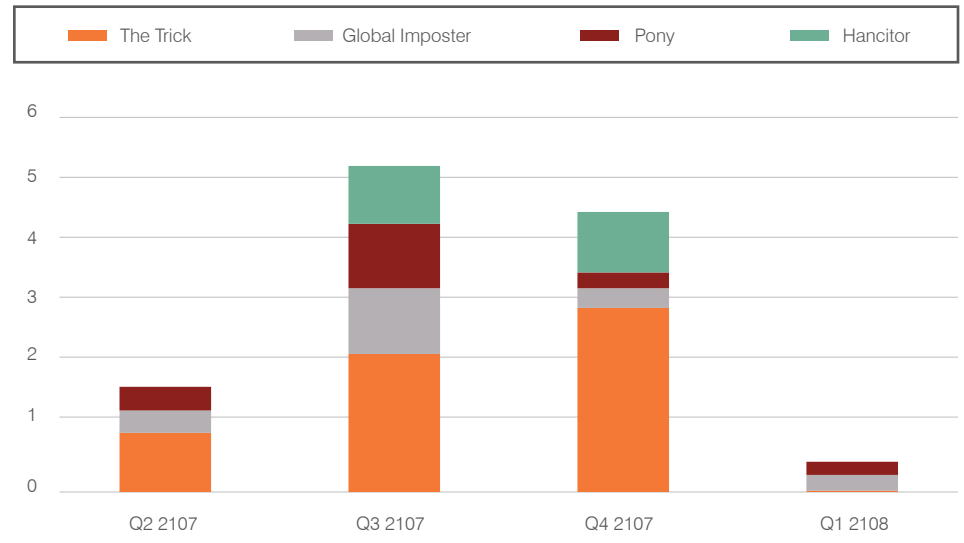


Figure 5: Top malware families

THE USUAL SUSPECTS: HEALTHCARE'S BIGGEST MALWARE THREATS

LOCKY	**Locky is a highly advanced form of ransomware adept at disguising itself.** Locky uses social engineering to trick users to download the ransomware, which locks and encrypts a large number of systems and file types.
THE TRICK	**The Trick is a clever banking trojan that "tricks" payment systems to redirecting to a counterfeit site** with a correct URL and a seemingly genuine digital certificate.
GLOBAL IMPOSTOR	**Global Impostor, also known as Fake Globe, mimics and is named after an earlier ransomware strain called Globe.** Initially used in small regional campaigns, GlobeImposter became a global threat when a prolific attacker known as TA505 began using it in larger campaigns.
PONY	**Pony is a Trojan that usually spreads through spam campaigns.** It hides PDF or Microsoft Office document. The spam messages typically mention a money transfer or overdue invoice notice to prod recipients to act right away. Pony disguises its code to stay hidden from many security tools.
HANCITOR	**Hancitor (also known as Chanitor or Tordal) is a malware downloader that spreads through malicious Microsoft Word macros sent in spam campaigns.** Though fully patched systems should be immune, attackers use social engineering to trick people into enabling macros on their system and running the malicious code.

MALWARE DELIVERY PREFERENCES: URLS VS. ATTACHMENTS

Most malware is delivered through file attachments or URLs that link to the malicious code. Which method attackers choose hinges on their tactics, available infrastructure, targets, cybersecurity defenses, and more.

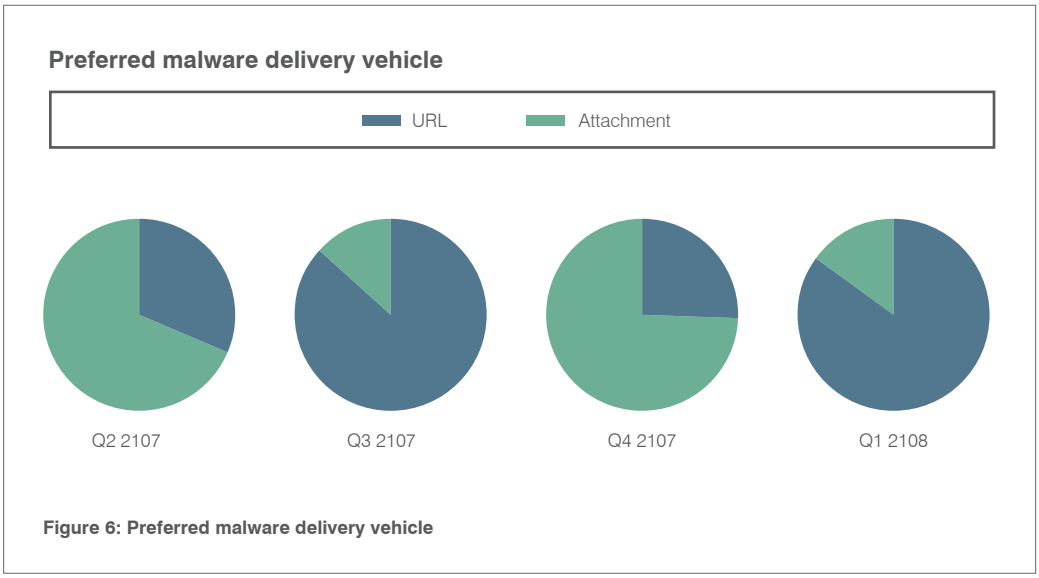


Figure 6: Preferred malware delivery vehicle

PROTECTED HEALTH INFORMATION IS VALUABLE TO CYBER CRIMINALS, WHICH MAKES HEALTHCARE A TOP TARGET.

For the last three quarters of 2017, we saw a combined average of 36 million malicious URLs and attachments being sent to healthcare companies. But by the first quarter of 2018, this number had plunged to just 8 million.

Is this the end of ransomware as a healthcare threat? Not likely. A more plausible explanation is that cyber criminals have switched to other techniques such as email fraud.

EMAIL FRAUD

Protected health information (PHI) is valuable to cyber criminals, which makes healthcare a top target. The industry's complex, expansive supply chain provides openings to use email to commit wire-transfer fraud and steal important data.

"Spear phishing" and broad-scale consumer phishing techniques are two forms of email fraud. Clinical staff, health consumers and business associates are all targeted.

Phishing techniques we observed in our study include:

- Domain spoofing—using someone else's trusted domain to send malicious messages
- Display-name spoofing—impersonating a person familiar in the email's "From" field to the message receiver to fool the recipient into thinking that the message came from a trusted source
- Lookalike (or cousin) domains—registered domains that look confusingly similar to a trusted domain. For example, registering "y0urdomain.com" to impersonate "yourdomain.com." This approach is also known as typosquatting.

WORDS THAT WORK: TOP SUBJECT LINES

Figure 7 shows the top subject lines used in fraudulent emails.

NEARLY 1 IN EVERY 5 EMAILS FROM HEALTHCARE-RELATED DOMAINS APPEARED TO BE FRAUDULENT.

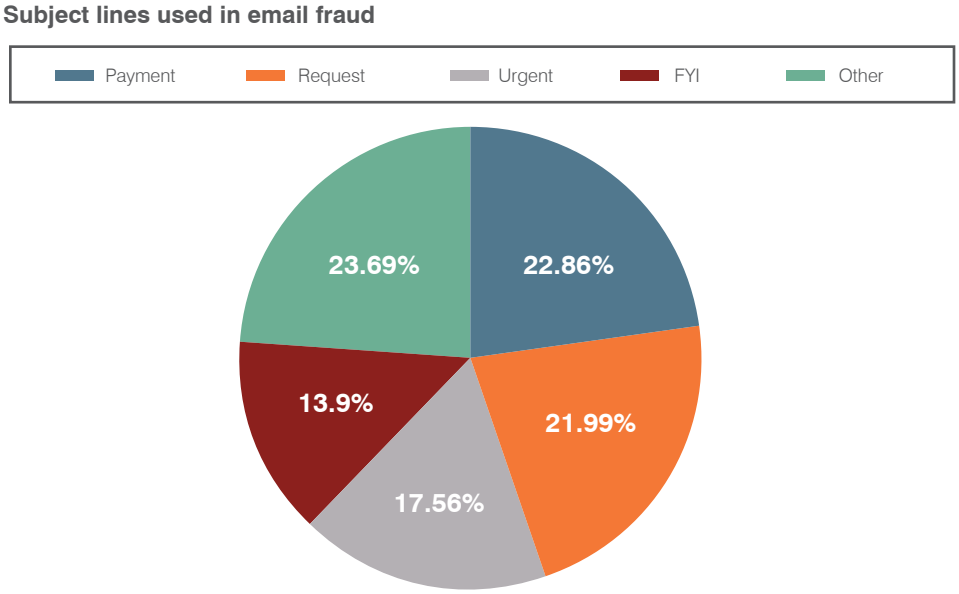


Figure 7: Subject lines used in email fraud

DOMAIN SPOOFING: A CLOSER LOOK

Domain spoofing is a popular tactics of email fraudsters. By exploiting a fundamental vulnerability of SMTP mail, attackers can build believable phishing scams. These attacks impersonate hospital personnel to deliver malicious attachments and non-malware threats such as email fraud.

We analyzed 3.1 billion emails that used the domain of a known healthcare brand during the study period. About 8.3% of these were actually from sources that were either unauthorized or malicious. The ratio might seem small, but it amounts to 262 million emails from a trusted domain. Recipients, even technically savvy ones, have no way of knowing who's really sending it. That's adds up to a huge problem for most health organizations.

When including other techniques such as display-name and lookalike spoofing, the percentage of suspected fraudulent emails rises to 18.2%—nearly 1 in every 5 emails.

LOOKALIKE DOMAINS

In lookalike (or cousin) domain spoofing, the attacker registers a domain confusingly similar to a trusted domain. It's an effective tactic that bypasses email authentication technology. That's because technically, the attackers aren't using anyone else's domain—they're using a domain that belongs to them but looks like someone else's. Many users don't notice the difference, lulling them into a false sense of security. Thinking they're dealing with someone they trust, users wire money, hand over valuable information, and more.

Attackers craft these lookalike domains by making small, hard-to-notice changes to the domain they're copying. They may swap out individual characters, such as the numeral 0 in place of the letter O. Or they may insert characters, such as adding an S at the end of the domain.

MANY USERS DON'T NOTICE THE DIFFERENCE, LULLING THEM INTO A FALSE SENSE OF SECURITY.

Like other email fraud tactics, lookalike domain techniques change all the time. But across 2017, swapping individual characters was the most popular, occurring nearly 38% of the time. Figure 8 shows the most common substitutions.

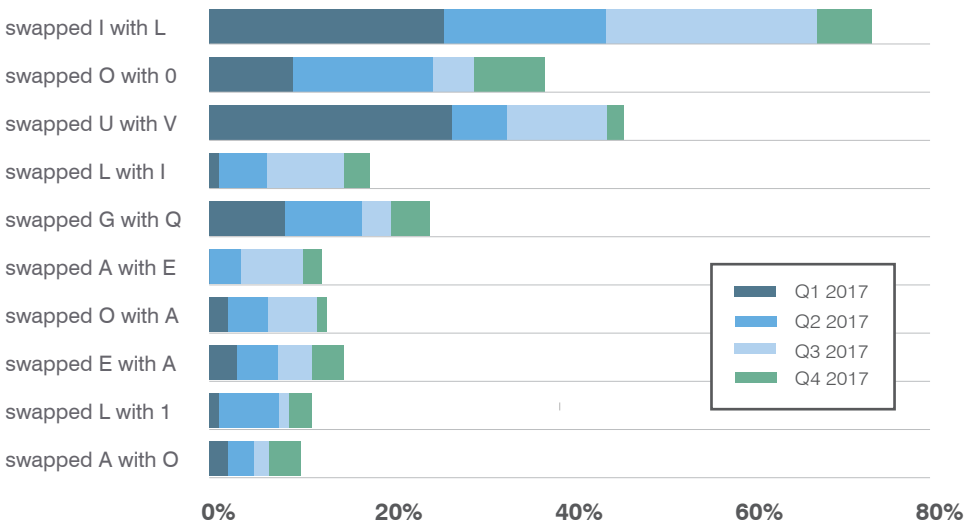


Figure 8: Top character swaps

The volume of lookalike domain attacks is not as high as display-name and domain spoofing. That's probably because this technique requires the attacker to register a domain, which costs money. But given that a single trusted domain name could have countless similar-looking variations, attackers have many openings to launch such attacks.

TAKING OFF THE KID GLOVES: ATTACKS TARGET PEDIATRICS

We saw many emails that targeted executives in some of the nation's most prestigious pediatric care hospitals. We saw an unusually high use of advanced attacks, such as credential phishing, whaling attacks, and crypto mining against this segment.

Why attackers would target this segment of healthcare in disproportionate numbers is unclear. Perhaps the specialized nature of their work puts the hospitals and their leaders in the public eye.

Here are some topics and subject lines that stood out:

- ICD-10 cash reserves
- Procedure authorization
- PDS inquiry
- Transaction completion

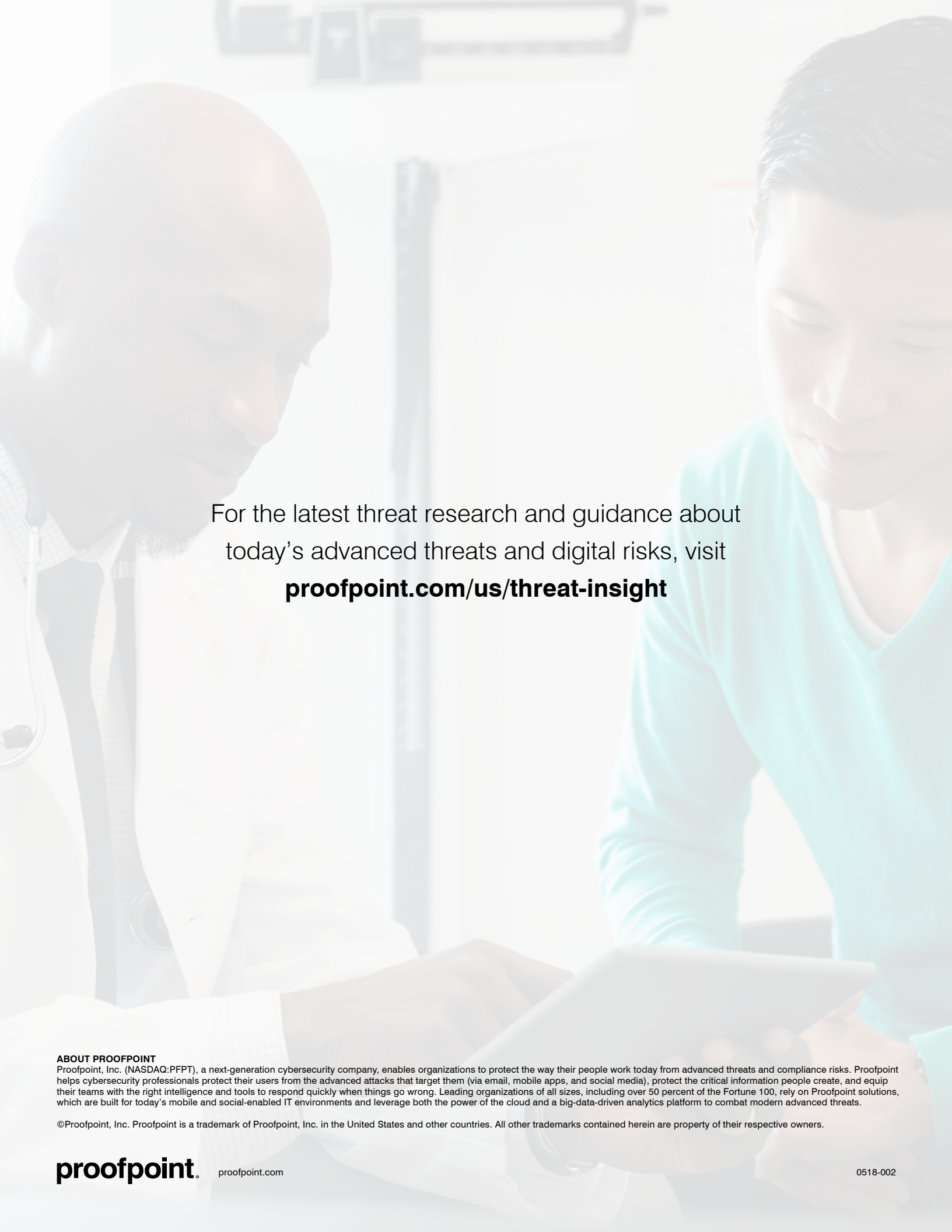
We also saw a high instance of business associates being impersonated, including dentists, surgical groups, orthopedic partners, and more.

RECOMMENDATIONS

Today's attacks target people, not just technology. They exploit the human factor: healthcare workers' natural curiosity, accute time constraints and desire to serve. Protecting against these threats requires a new, people-centered approach to security.

We recommend the following:

- **Prepare for more ransomware attacks**. Ransomware is still lucrative for threat actors in broad-based campaigns. Attackers tend to rely on high volumes and ransoms within the reach of potential victims to monetize ransomware. But healthcare organizations are becoming a favorite for more targeted, higher-ransom attacks.
- **Train your people to spot attacks that target them.** Your security awareness training should include phishing simulations that use real-world tactics to see who's most at risk. Teach them to recognize attacks on email, cloud apps, mobile devices, the web, and social media.
- **Get advanced threat analysis that learns and adapts to changing threats.** Today's fast-moving, people-centered attacks are immune to conventional signature- and reputation-based defenses. Be sure your defenses adapt as quickly as attackers do.
- **Deploy DMARC authentication and lookalike domain (typosquatting) defenses.** These technologies stop many attacks that use your trusted brand to trick employees, partners, vendors, and customers.
- **Get visibility into the cloud apps, services and add-ons your people use.** Deploy tools to detect unsafe files and content, credential theft, data theft, third-party data access, and abuse by cloud scripting apps.
- **Automate some aspects of detection and response.** Automated tools can proactively detect security threats and other risks posed by the ever-growing volume of apps your people use in the enterprise. And security orchestration and automation solutions can help you respond faster and more effectively. Consider solutions that connect, enrich, and automate many steps of the incident response process. That frees up security teams to focus on tasks that people do best, boosting awareness and security.



For the latest threat research and guidance about today's advanced threats and digital risks, visit **proofpoint.com/us/threat-insight**

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.