



2019 PHISHING AND FRAUD REPORT

**Simple Yet Effective Attacks
You Can't Afford to Ignore**

AUTHORS:

David Warburton and Raymond Pompon

CONTRIBUTORS:

Webroot | CI Security | F5 Security Operation Center



CI Security™



Introduction

Welcome to F5 Labs' third annual report on phishing and fraud. Once again, we're bringing you data from our partner Webroot as well as the F5 Security Operations Center.

Phishing continues to be a major source of profit for cyber-criminals, and a big hassle for cyber-defenders. In the F5 Labs [2019 Application Protection Report](#), F5 Labs found that phishing was responsible for 21% of breaches, the second largest cause of breach reported by U.S. companies. The number one reported breach cause (absent other details) was unauthorized access to email. Because phishing can commonly grant unauthorized access to email, it's likely phishing is also the cause of some of these breaches. So there you have it: one of the most prevalent ways attackers are breaching data is via phishing.

ONE OF THE MOST PREVALENT WAYS ATTACKERS ARE BREACHING DATA IS VIA PHISHING.

Anyone who's been reading our reports over the years should not be surprised by this, since phishing has been bouncing into the top spot every time we look at breach causes. Speaking of breach causes, the 2019 Application Protection Report showed that the finance, health, education, non-profit, and accounting sectors were significantly more likely to be compromised through phishing or illicit email access than any other means.

Why so much phishing? The reason is simple: it's easy and it works. Attackers don't have to worry about hacking through a firewall, finding a zero-day exploit, deciphering encryption, or rappelling down an elevator shaft with a set of lockpicks in their teeth. The hardest part is coming up with a good trick email pitch to get people to click on, and a fake site to land on.

The Extant State of Phishing Attacks

It's 2019 and we're still dealing with phishing, which stretches back 25 or more years.

Mike Simon, CTO of managed detection and response firm CI Security, sees a lot of security incidents. We asked him what he thought of the current state of phishing attacks.

He told us:

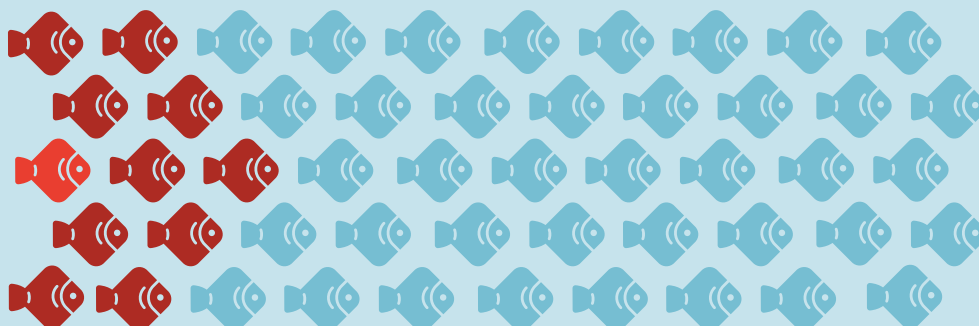
“Broad, historic data on network activities are critical to dealing with phishing. Because CI Security gathers and indexes a broad spectrum of information about activities on customer networks, the question we asked ourselves was around how that information might be useful in reducing the potential impact of phishing in an organization.

As it turns out, our data shows that phishing emails are almost like cockroaches in a lot of ways. If you see one, there are thousands more that are not in plain sight, but doing damage.

“If someone in the organization receives a phishing email and reports it, our testing shows that somewhere between 15% and 20% of the organization received the same phish; and depending on timing, possibly some before it was recognized. It is important at that point to be able to verify if any of the artifacts embedded in the known phish have been active on the network.”

“IF SOMEONE IN THE ORGANIZATION RECEIVES A PHISHING EMAIL AND REPORTS IT, OUR TESTING SHOWS THAT SOMEWHERE BETWEEN 15% AND 20% OF THE ORGANIZATION RECEIVED THE SAME PHISH.”

MIKE SIMON, CTO, CI SECURITY



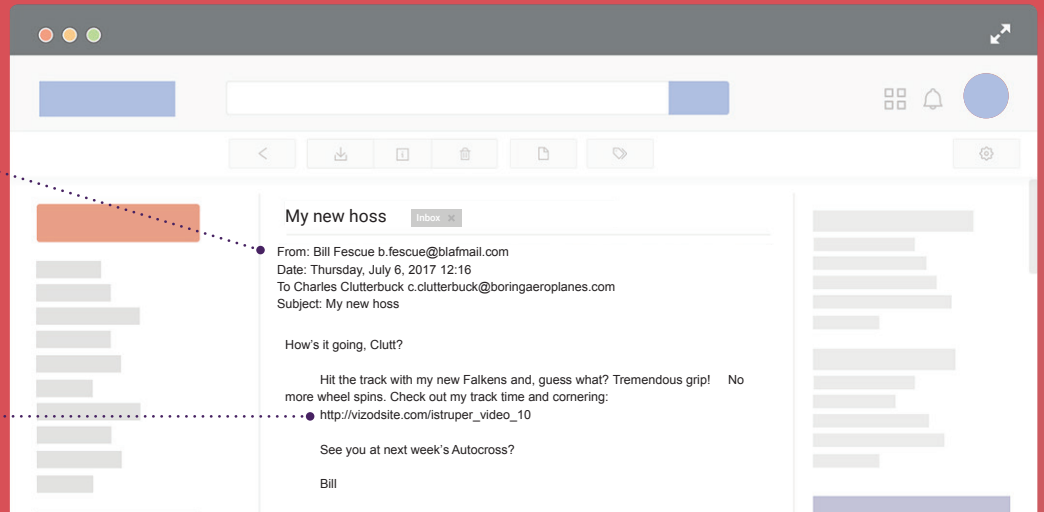
Anatomy of a Phishing Attack in 2019

There's plenty of phish in the sea... er, Internet, so let's debone an aggregate phishing attack and take a look. Webroot gave us a detailed snapshot of phishing data for the month of July 2019, which we sliced and tweezed apart to show you what's going on in phishing.

FIGURE 1
ANATOMY OF A PHISHING ATTACK

Fake name could be created based on open source intel (social media) analysis of target's friends/colleagues.
Email address and name discovered via open source intel or purchase of spam lists.

Phishing emails are three times more likely to have a malicious link than a malicious attachment.



85% of phishing sites tested use certificates signed by a trusted Certificate Authority (CA); 17% made use of self-signed certificates. Many certs had alternative names, allowing for multiple re-use of the same certs.

36% of phishing sites had certs lasting only 90 days, suggesting the use of cert automation services such as LetsEncrypt.



71% of phishing sites use HTTPS to appear more legitimate.

The most impersonated brands or sites are Facebook, Microsoft Office Exchange, and Apple.

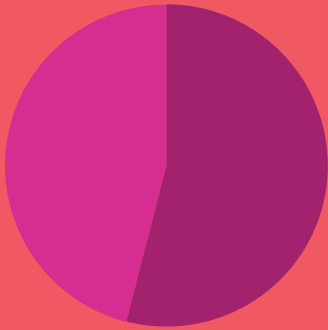
Top domains featuring unique phishing sites include blogspot.com, 000webhostapp.com, ebaraersc.net, and .info.

TARGET EMAIL ADDRESSES

Target addresses for phishing emails come from a variety of sources, such as spam lists and open source intelligence gathering. Depending on the targeting of victims (who attackers are going after and how hard), phishing emails could be sent out to thousands of potential victims or just one. For more information on address collection methods, see the [F5 Labs 2018 Phishing and Fraud Report](#).

THE PHISHING EMAIL ITSELF

As Mike Simon from CI Security mentioned earlier, 15% to 20% of the organizations they manage security responses for receive the same phishing email across multiple users. What do these emails look like? Well, most of them are links that lead to fake websites. In our 2018 Phishing and Fraud Report, Webroot found that phishing emails were three times more likely to have a link to a malicious site rather than an attachment containing malware.



54%

OF MALWARE DOMAINS
LEVERAGED HTTPS
IN JULY 2019

MALICIOUS LINKS LEAD TO FAKE WEBSITES

Those malicious links lead right to fake websites designed to harvest credentials, trick the victim into installing malware, or inject drive-by exploits into vulnerabilities in the user's browser. What do they look like? Again, as we pointed out in our 2018 report, phishers prefer to impersonate popular brands or platforms in their phishing websites. The top faked sites were, in order: Facebook, Autodiscover (used by attackers to try to steal credentials from Microsoft Outlook sessions), Apple, Chase, Office, WhatsApp, Paypal, Amazon, Microsoft, Netflix, iCloud, and Office365.

THE TOP FAKED SITES WERE, IN ORDER: FACEBOOK, AUTODISCOVER, APPLE, CHASE, OFFICE, WHATSAPP, PAYPAL, AMAZON, MICROSOFT, NETFLIX, ICLOUD, AND OFFICE365.

The fake phishing sites are hosted across a wide range of hosts on the Internet, but the most prevalent domains are 4cn.org (2.7%), airproxyunblocked.org (2.4%), 16u0.com (1.0%), and prizeforyouhere.com (1.0%). As for where specifically, Blogspot.com sites captured the top slots for both phishing (4%) and malware (43%) sites.

And, what kinds of tricks were the phishers trying to pull? The most frequently appearing patterns in the examined phishing URIs were .htm (19.4%), .php (7.4%), login (3.0%), and admin (1.2%).

ENCRYPTION DISGUIISING A SUCCESSFUL MALWARE CAMPAIGN

In the 2018 Phishing and Fraud Report, F5 Labs analyzed malware domains collected by Webroot that were active in September and October of 2018 and found that 68% listened on port 443. F5 Labs analyzed another sample of malware domains from Webroot that were active in July 2019 and discovered 54% of them were listening on port 443. Leveraging HTTPS encryption to hide malware from traditional intrusion detection systems (IDSs) is a common threat actor tactic, and one we are seeing increase and decrease in line with the overall attack trend (see Figure 3 on page 7). The majority of malware cannot be detected without SSL/TLS inspection.

7%

OF PHISHING SITES USE
NON-STANDARD TLS PORTS

REAL CERTIFICATES ON REAL PHISHING SITES

Not only are a majority of phishing sites encrypted, but a majority of them are using legitimate certificates. We found only 17% of phishing sites used self-signed certificates, with many of those belonging to Windows IIS servers. The folks that are falling for these self-signed phishing sites are likely clicking through the browser certificate warning.

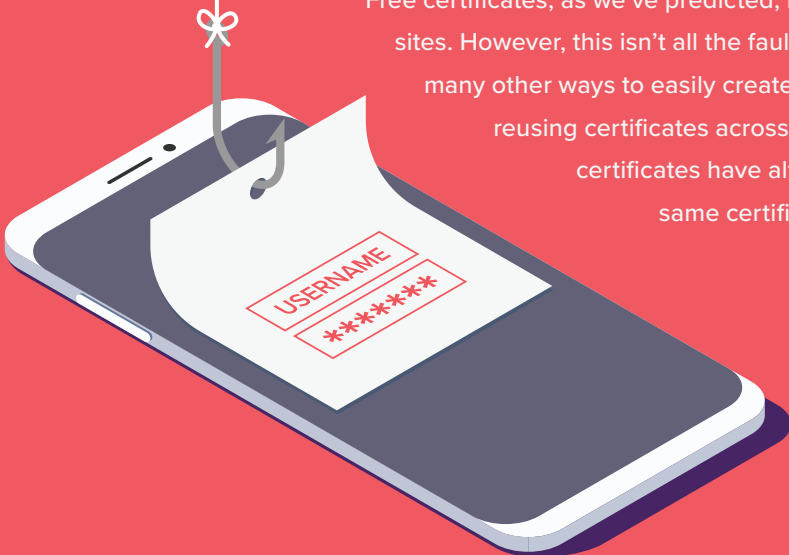
EVEN WORSE, 21% OF CERTIFICATES ON PHISHING SITES INCLUDE EITHER 20% ORGANIZATION VALIDATION (OV) AND 1% EXTENDED VALIDATION (EV) TYPES.

Even worse, 21% of certificates on phishing sites include either 20% Organization Validation (OV) and 1% Extended Validation (EV) types. The whole point of validated certificates is to provide assurance of an organization's ownership of a domain. It seems that this is not working out so well. In fact, two major browsers, Chrome and Firefox, have announced plans to take the display of Extended Validation off the main screen. Apple's Safari has already deprototyped them.

PHISHERS ARE GOOD AT THEIR JOBS

Because phishing is a "volume business," it makes sense that phishers embrace efficient methods, such as automation, to help manage their flock of fakes. The data shows that many phishing sites obtain certificates from cPanel (integrated with the Comodo CA) and LetsEncrypt (first and third place in popularity), and 36% of phishing sites had certs that lasted only 90 days. This strongly suggests that phishers are using certificate automation. This automation allows a phisher to programmatically orchestrate the process of purchasing and deploying certificates across all their domains and manage their expiration.


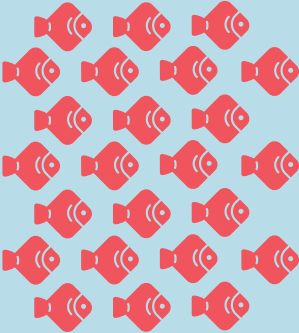
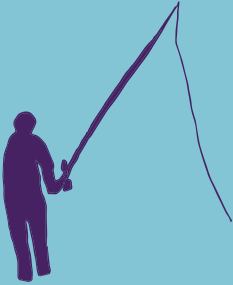
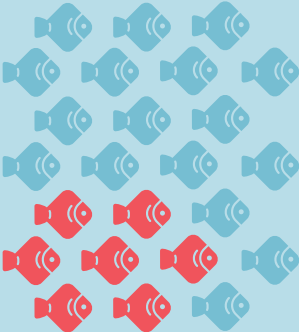

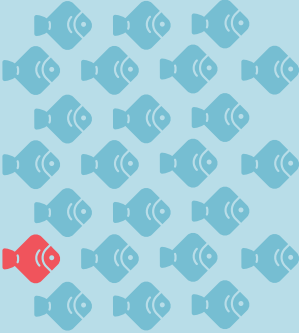
Free certificates, as we've predicted, make it much easier for attackers to host phishing sites. However, this isn't all the fault of LetsEncrypt, as some people believe. There are many other ways to easily create free TLS certificates. Phishers are being frugal and reusing certificates across phishing and malware sites. This is because many certificates have alternative names, allowing for multiple re-use of the same certificates across many domains.



Anatomy of a Phisherman

All kinds of attackers phish. From script kiddies to state-sponsored advanced attackers (also known as advanced persistent threat (APT) groups), phishing is the weapon of choice. Sometimes the plan is to hit a specific person; sometimes it's to target a group of people in an organization; other times the plan is just to aim at whoever takes the bait. It all depends on what attackers are going after and how much effort they're willing to invest. Here's a quick breakdown:

FIGURE 2
Anatomy of a Phisherman

<p>INDISCRIMINATE</p> 		<p>APPROACH</p> <p>“Spray and pray” against big list of email addresses</p> <p>GOAL</p> <p>One out of a thousand will bite: steal their credentials, or inject malware</p>	<p>BAIT</p> <p>Impersonate common tech brand (Microsoft, Google, Apple, Facebook)</p> <p>DEFENSE</p> <p>Mail filtering, security training, SSL inspection</p>
<p>SEMI-TARGETED</p> 		<p>APPROACH</p> <p>Targeted at a single organization of affinity group</p> <p>GOAL</p> <p>Phish members in the affinity group for fraud (e.g., group includes bank customers) or gain illicit network access (e.g., group includes an organization's users)</p>	<p>BAIT</p> <p>Impersonate service organization or department known to the target group (“Click here to get holiday bonus from HR;” invoice from vendor; resumé matching open jobs)</p> <p>DEFENSE</p> <p>All of the above plus threat intelligence to identify reconnaissance and early attempts in phishing campaign</p>
<p>SPEAR PHISHER</p> 		<p>APPROACH</p> <p>Targeted at a single individual (usually C-level or SysAdmin)</p> <p>GOAL</p> <p>High-dollar fraud (wire transfer, fake invoice); ransomware injection, theft of secrets</p>	<p>BAIT</p> <p>Impersonate someone known to targeted individual; leverage previous takeovers</p> <p>DEFENSE</p> <p>All of the above plus inspection filter, training, duties on high-value targets</p>

Phriends and Phamily Phishing

Attackers have recently adopted a tactic of using open-source intelligence (such as scraping social media) to identify a target's friends or family. Attackers then compromise those email accounts, giving them the ability to send phishing emails from legitimate, trusted addresses. This same trick can work within a company to target coworkers or customers. In the F5 Labs 2019 Application Protection Report, we found that 4% of email breach cases explicitly noted that attackers used a stolen mailbox to phish others within the same organization. This is a prevalent tactic when stealing research and intellectual property in educational institutions.

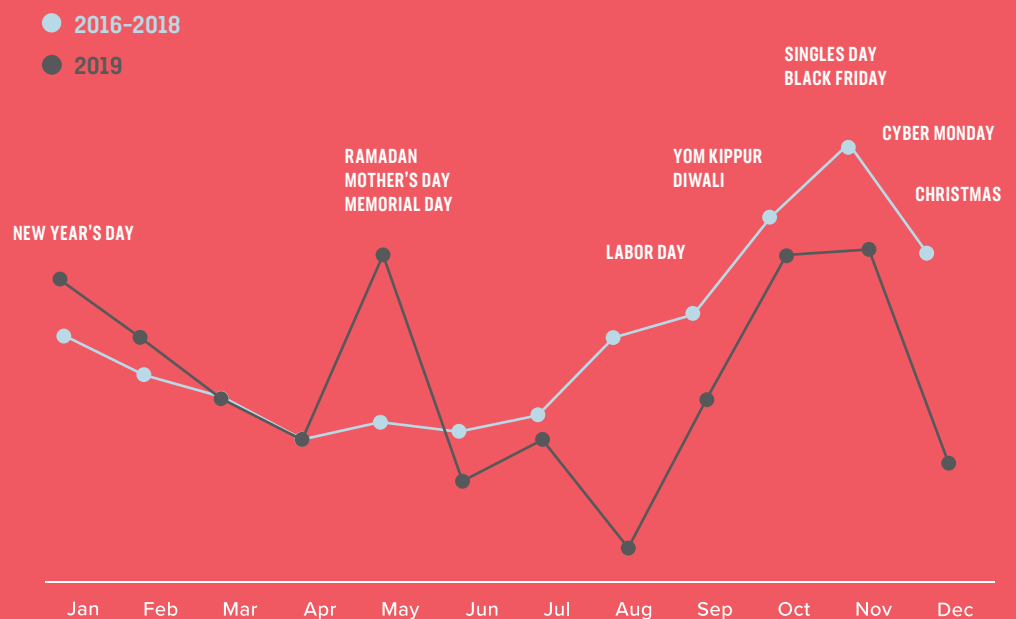
Phishing Trends

Does phishing have a season? Last year, we looked at three years worth of phishing attack data collected from the F5 SOC and discovered a 50% increase in phishing attacks during the "holiday" season (roughly October through January). This was expected behavior because it's easier to trick people into opening up package delivery notifications or receipt emails during the height of holiday shopping.

However, the past year of phishing hasn't shown the same pattern. The rise of social media makes personal data freely available to attackers anytime, so they don't have to wait for the end-of-year holiday shopping season to trick unsuspecting shoppers. As a result, we expect phishing to become a more balanced year-round sport. Looking at phishing trends in 2019, there is a spike in attacks in springtime, followed by another spike in the months leading up to end-of-year holidays and purchasing events, likely attributed to large cybercrime campaigns.

FIGURE 3
Phishing and fraud attacks, from September 2016 to September 2019.

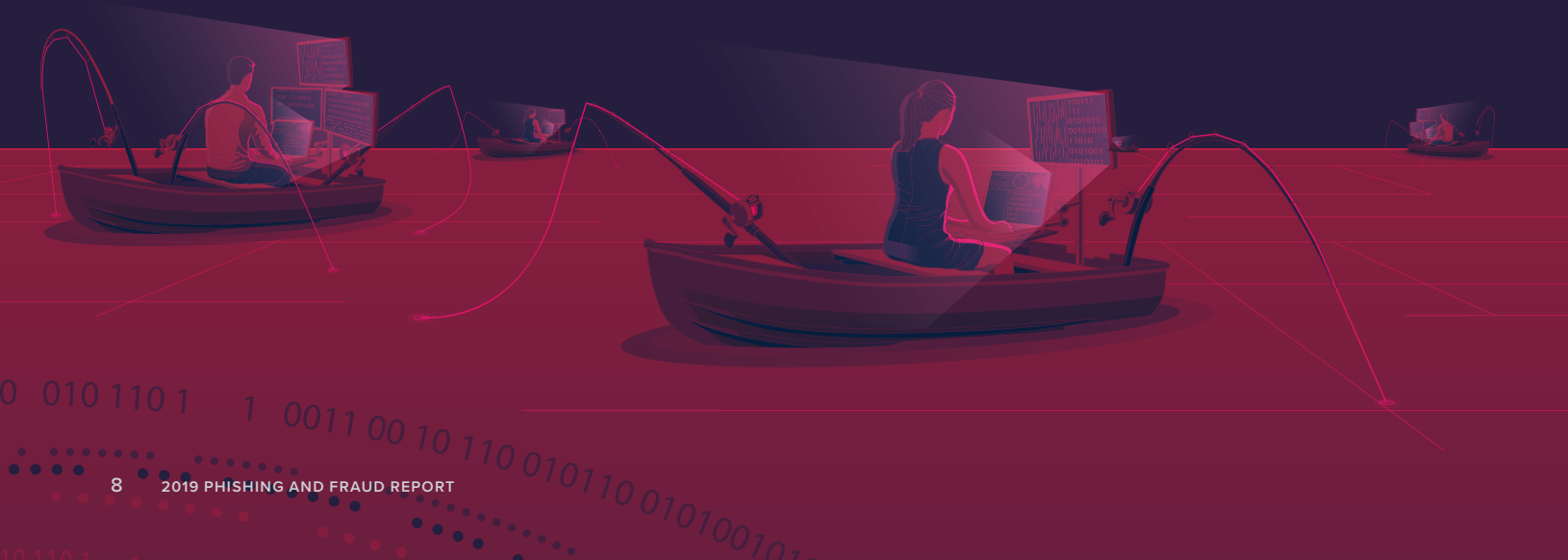
THE 2019 TREND SHOWS THAT PHISHERS ARE TAKING ADVANTAGE OF MORE HOLIDAYS THAN THEY DID IN THE THREE PRIOR YEARS.



Responding to Phishing

Every organization is on the receiving end of phishing attacks, whether they're discovered or not. Given the success rate of phishing and its status as the top root cause of breaches, every organization needs a phishing response. Such a strategy must include security awareness training, and the following technical [security controls](#):

- **Deploy multifactor authentication (MFA).** Employees will get phished. Credentials will get collected, and attackers will try to use them. MFA is your phishing “gap insurance,” preventing stolen credentials from being used from an unexpected location or unknown device.
- **Clearly label all email** from external sources to prevent spoofing.
- **Use antivirus (AV) software.** It is a critical tool to implement on every system a user has access to—most importantly, their desktop systems and laptops. In most cases, AV software will stop a malware installation attempt as long as the software is up to date, so set your AV policy to update daily, at a minimum.
- **Have a web filtering solution** in place to prevent users from inadvertently visiting phishing sites. When a user clicks on a link to a phishing site, this solution will block that outbound traffic.
- **Inspect encrypted traffic for malware.** Traffic from malware communicating with command and control (C&C) servers over encrypted tunnels is completely undetectable in transit without some kind of decryption gateway. Since the majority of malware phones home over encrypted tunnels, you need to decrypt your internal traffic before sending it through your incident detection tools to detect infections.
- **Make it easy for users to report phishing.** If 15 to 20% of the organization receives the same phishing email, then incident response should include a streamlined and guiltless method for users to report suspected phishing.
- **If people are clicking on phishing email links, get visibility** with endpoint monitoring into what's going on, what malware is becoming active on your network, and what credentials may be compromised.





APPLICATION THREAT INTELLIGENCE



US Headquarters: 801 5th Ave, Seattle, WA 98104 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com

©2019 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of the respective owners with no endorsement or affiliation, expressed or implied, claimed by F5. RPRT-SEC-405279820 | 10.19