



THE WEAKEST LINK?

SOLVING SUPPLY CHAIN PHISHING ATTACKS

The Weakest Link: Your Partners

Hackers have goals. Whether the goal is to steal data, earn financial rewards, manipulate information, or cause physical destruction, attackers don't limit themselves to a direct attack on their target victim. Instead, they often use their imaginations and go after the digital supply chain of their targets as well. Hackers can do this without increasing the need for technical sophistication, and without risking or compromising the success of their campaigns.

Digital supply chain attacks exploit an organization's reliance on suppliers, partners, and vendors to [find and prey on the weakest links in the chain](#). Suppliers, partners, vendors, and affiliates hold sensitive data; their IT infrastructure is typically less secure, or is ineffectively defended and can serve as a stepping stone, providing surreptitious opportunities to hackers for enhancing their phishing campaigns.

Many prominent campaigns have been the result of supply chain phishing:

		
WHAT: The Anthem Breach	WHAT: The Target data breach	WHAT: The Home Depot data breach
78 MILLION DATA RECORDS EXPOSED	40 MILLION CUSTOMER CREDIT CARD NUMBERS EXPOSED	56 MILLION CUSTOMER CREDIT CARD NUMBERS EXPOSED
HOW: A phishing attack within a subsidiary partner of Anthem	HOW: Attackers initially gained access to the network using credentials obtained from heating, ventilation, and air-conditioning (HVAC) subcontractor Fazio Mechanical Services, via a phishing attack	HOW: A supply chain phishing attack where a third party vendor's username and password were used to enter the Home Depot's network

Supply Chain / Account Takeover Attacks: Trust, but Verify

Area 1's unique insight into global campaigns and associated analytics of emergent phishing attacks allows us to protect our customers against these supply chain / partner originated phishing attacks.

A common tactic used by attackers is to take over accounts within partner organizations; and use that as leverage to breach the primary organization. This creates a natural entryptpoint for attackers to get inside the organization since partner communications are usually trusted; and often times are bypassed from secondary inspections within the customer.

In order to detect these, Area 1 employs a diverse set of analytics to understand the authenticity of the message across the **7** different supply chain phishing use cases seen:

1

Compromised Partner IP / Domain space:

Using our extensive crawling abilities and insight into global email traffic, Area 1 has prior knowledge of known good organizations, domains and IP addresses that are compromised at any given point of time; and are sending suspect messages and emails out. As they traverse through our filters, Area 1's verdict engine will flag and stop these messages from going through.

2

Compromised Partner Accounts:

Area 1 maintains a continuous and dynamic list of email accounts and domains that are sending out phishing campaigns; irrespective of the authenticity of the organization. These could include valid organizations / businesses that are compromised by threat actors, organizations that act as a front for threat actors or organizations that are owned by threat actors. In any of these use cases, messages coming from these accounts will be flagged as a phish even if its impersonating a partner.

3

Compromised Accounts, URL Campaigns:

Attackers will use the partner's domain to send a Phish message, with a call to action that typically hosts a credential harvester, or a malicious payload. Irrespective of whether it gets sent by a trusted partner, Area 1's verdict engine enforces a range of checks to assess the veracity of the message:

- Preemptive and instant crawling of the URLs and associated domains
- Malicious payload analytics and active content detection within the URLs
- Enhanced Computer Vision analytics and Brand detections on form submission pages to detect active Credential Harvesters.
- Link shortener analysis and deep link follow throughs to assess eventual landing points of the CTA pages.

[Continued on Next Page](#) →

In order to detect these, Area 1 employs a diverse set of analytics to understand the authenticity of the message across the **7** different supply chain phishing use cases seen:

4

Compromised Partner Accounts, New Domain campaigns:

A recurring tactic for attackers is to leverage new domains to send out campaigns or reference new domains within the phishing message for a campaign that comes from a compromised partner. **Area 1 is unique in its ability to combine domain age of any or all elements within the message** and use it either as a singular determining factor (many of our highly security conscious customers choose to do this) or as one of many factors while determining if the message is valid or not. Attackers using this tactic consistently get caught even if they are sending messages from a valid partner.

5

Compromised Partner Accounts, Malicious payloads / invoices:

Another popular method is to compromise a partner, especially a financial or a payment partner and leverage a known user name to send out malicious or fake invoices for payment. These invoices could contain an active payload (such as VBA, PE, EXE etc.) to breach the partner, or link to a fake invoice payment site luring the user to part with their credentials or make an inadvertent payment. **Area 1's payload analytics on the attachments and URL analytics on the link** catches these campaigns irrespective of the source / origin of the campaign.

6

Compromised Partner Accounts, Partner BEC:

Business Email Compromise or Executive impersonation attacks have skyrocketed in recent years. A new variation of this technique is Partner BEC attacks where the message originates from a valid partner that's compromised, has no payload (file or URL) and impersonates a trusted colleague or executive at the partner site. **Area 1 utilizes multi-variate analytics that parse the targeted user, sender, intent, urgency, word count, time stamps along with a combination of proprietary keyword dictionaries** to surface if the message is a Partner BEC or a valid request.

7

Partner Spoofing:

Often times, attackers may not have actually compromised a partner but may spoof a partner through a variety of techniques to lure unsuspecting users. This could be through a domain spoof or registering look alike partner domains to trick the recipient into interacting with the message. **Area 1's service uniquely combines cousin domain / look alike domain detection that extends to partner domains as well,** along with employing enhanced Sender Verification techniques that go beyond traditional Email Authentication checks employed the industry.

THERE MUST NOT BE A WEAK LINK IN YOUR ENTERPRISE SECURITY ECOSYSTEM.

To learn more about extending phishing protection outside your network throughout your digital supply, visit www.area1security.com or contact info@area1security.com today.

Compromised Partner: URL + Malicious Payload Campaign

In the Summer of 2017, Iranian hackers identified by Area 1 Security as IRN2 and previously referred to as “OilRig” compromised a supplier website belonging to Doosan Power Systems India (DPSI) to conduct a targeted phishing campaign against

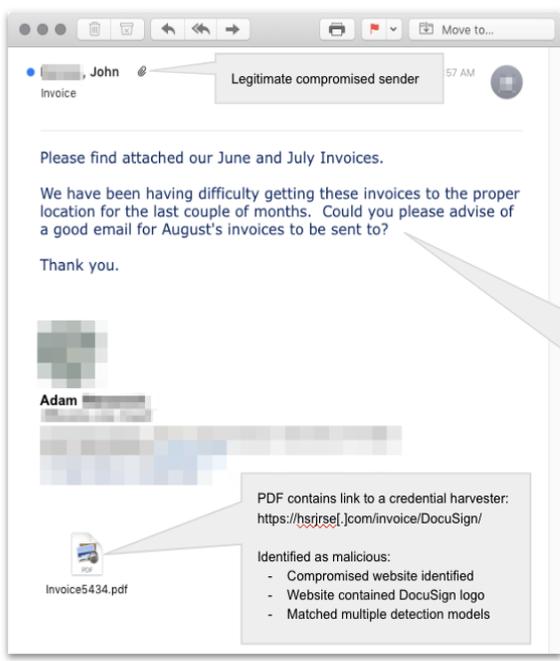
Saudi Aramco. This campaign used a career-themed, socially engineered phishing attack. Iranian hackers compromised DPSI’s website, a trusted, legitimate domain, to host a weaponized, encrypted, password-protected .zip archive.



Unsuspecting Saudi Aramco targets received an email inviting them to apply for a position at DPSI. Victims then clicked a link in the email, whereupon a password-protected .zip archive downloaded to the target’s system, surreptitiously installing malware, a variant of the Helminth backdoor. This executed on the victim’s system, creating an entree for attackers to the Saudi Aramco network. The download also launched a DPSI career page, a fake phishing website, inviting the victim to register an account and submit a resume. This ploy minimized the victim’s suspicions and collected more potentially sensitive information, including credentials, that attackers could use for additional socially engineered lures and malicious attacks.

Compromised Partner: Fake Invoice, URL Campaign

Example of a compromised partner's account being used to phish using a fake invoice lure.



Trusted customer has their account compromised and sends a fake invoice to an Area 1 customer.

Message defeats email authentication and passes SPF, DKIM and DMARC checks.

```
Authentication-Results: [redacted]; spf=None
smtp.pra=[redacted]; spf=Pass
smtp.mailfrom=[redacted]; spf=None
smtp.helo=postmaster@us-smtp-delivery-161.[redacted]; dkim=pass
(signature verified) header.i=@[redacted]
```

X-[redacted]-Dmarc-Check-Result: validskip

Lexical analysis algorithms and models used to identify message sentiment. Words in the messages are weighted to identify the intention of the message.

Cross validation with the malicious content of the PDF confirms malicious disposition

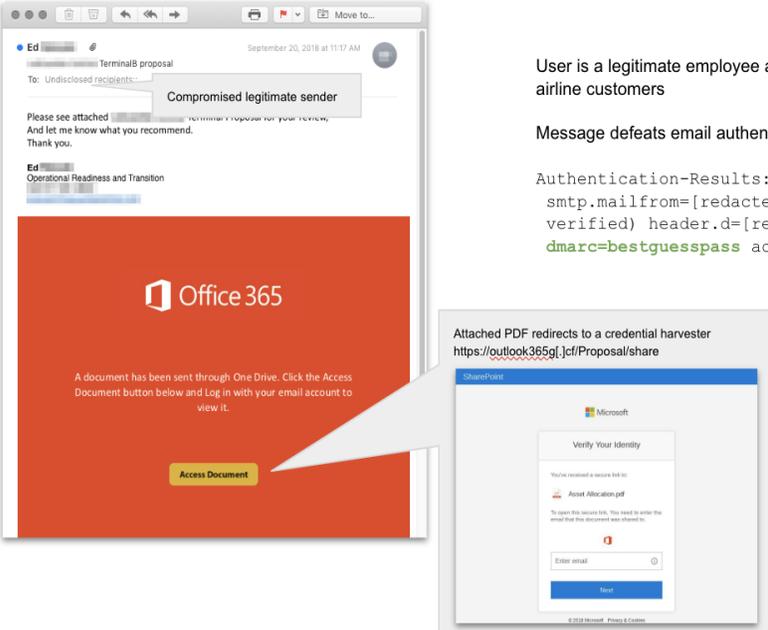
PDF contains link to a credential harvester:
<https://hsjrsej.com/invoice/DocuSign/>

Identified as malicious:

- Compromised website identified
- Website contained DocuSign logo
- Matched multiple detection models

Compromised Partner: URL Campaign, Credential Harvester

Example of a compromised partner's account being used to phish using an Office 365 credential harvester.



The image shows a screenshot of an email client interface. The email is from 'Ed [redacted]' with the subject 'TerminalB proposal' and is dated 'September 20, 2018 at 11:17 AM'. The recipient is 'Undisclosed recipients:'. The email body contains a red banner with the Office 365 logo and the text: 'A document has been sent through One Drive. Click the Access Document button below and Log in with your email account to view it.' Below the banner is a yellow 'Access Document' button. A callout box points to the button with the text: 'Attached PDF redirects to a credential harvester https://outlook365gl.jcf/Proposal/share'. To the right of the email screenshot, there is a text box with the following text: 'User is a legitimate employee at a tier 1 airport, attempting to phish one of our airline customers' and 'Message defeats email authentication, passes SPF, DKIM, and DMARC'. Below this text is a code block showing authentication results: 'Authentication-Results: spf=pass (sender IP is 104.47.40.57) smtp.mailfrom=[redacted]; dkim=pass (signature was verified) header.d=[redacted].onmicrosoft.com; dmarc=bestguesspass action=none header.from=[redacted];'. Below the code block is a screenshot of a 'Verify Your Identity' page from Microsoft. The page has the Microsoft logo and the text: 'You've received a secure link to: Asset Allocation.pdf'. It asks the user to open the secure link and enter their email address. There is an input field for 'Enter email' and a blue 'Next' button. At the bottom, it says '© 2018 Microsoft. Privacy & Cookies'.

User is a legitimate employee at a tier 1 airport, attempting to phish one of our airline customers

Message defeats email authentication, passes SPF, DKIM, and DMARC

```
Authentication-Results: spf=pass (sender IP is 104.47.40.57) smtp.mailfrom=[redacted]; dkim=pass (signature was verified) header.d=[redacted].onmicrosoft.com; dmarc=bestguesspass action=none header.from=[redacted];
```

Attached PDF redirects to a credential harvester
<https://outlook365gl.jcf/Proposal/share>

Compromised Partner: Malicious Payload

Example of a compromised partner's account being used to phish using a malicious payload hosted at a legitimate hosting provider.

Compromised business partner sender account

Dear Margaret [redacted], I spoke with Paul [redacted], your head office chief from [redacted] and need to notify you of the **termination of an employment contract. Please download it here and review.** (not available on mobile devices, only for the Desktop Computers).Margaret, please review it before i will call you back again.

Stephanie [redacted], Executive Lawyer
[redacted]

Passes both SPF and DKIM, no DMARC records defined for this domain.

Authentication-Results: **spf=pass** (sender IP is 149.72.158.248) smtp.mailfrom=sendgrid.net; **dkim=pass** (signature was verified) header.d=sendgrid.net; dmarc=none action=none header.from=[redacted];compauth=fail reason=001

Known good link used to download a malicious executable file

About Area 1 Security

Area 1 Security is the first to bring accountability to cybersecurity. Backed by top-tier investors, Area 1 Security is led by security, Artificial Intelligence, and data analytics experts who created a preemptive solution to stop phishing, the number one cause of cyber attacks.

Area 1 Security works with organizations worldwide, including Fortune 500 banks, insurance, and tech companies, and healthcare providers to realign their cybersecurity posture for combating the most significant risks, protecting customer data, and stopping attacks before they happen. Area 1 Security is a recipient of Inc. Magazine's "2018 Inc.'s Best Workplaces" in America. To learn more about Area 1 Security, visit www.area1security.com, join the conversation at [@area1security](https://twitter.com/area1security) or follow the [blog](#) for the latest industry news and insights on how to stop phishing.

► [Learn More](#) INFO@AREA1SECURITY.COM