

Hooking the Spear-phisher

Methods for investigating Business Email Compromises

by **SecurityScorecard's STRIKE Team**



[SecurityScorecard.com](https://www.SecurityScorecard.com)
info@securityscorecard.com

Tower 49
12 E 49th Street
Suite 15-001
New York, NY 10017
[1.800.682.1707](tel:18006821707)

Overview

In August 2022, SecurityScorecard was the target of a spear-phishing campaign involving two attacks. The first attack was an email claiming to be from SecurityScorecard's Co-Founder and CEO. The email domain, however, was not known to or registered by SecurityScorecard. The second attack involved emails impersonating a vendor targeting SecurityScorecard employees.

Vigilant employees alerted SecurityScorecard's Threat Research, Intelligence, Knowledge & Engagement (STRIKE) team, and they moved immediately into action. Not only was the STRIKE team successful in stopping the attack, but they also conducted a counter-offensive operation, exposing the attackers' IP address and estimated location and shutting down the bank account associated with their operation.

This paper outlines the methodologies used by STRIKE to successfully defend against this attack, gain additional intelligence, and deny the threat actors use of its infrastructure. This paper is also intended to serve as a guide for security operations and threat hunting teams who wish to learn more about methods and tools they can leverage when conducting similar investigations for their organization.

Initial Attack & Compromise

In early August, a series of emails were sent to several employees in SecurityScorecard's accounting department. The emails were designed to appear as if they were sent from Aleksandr Yampolskiy, SecurityScorecard's Co-Founder and CEO. Employing clever social engineering techniques, the emails asked recipients to provide a list of SecurityScorecard's vendors and billable accounts. Unfortunately, one recipient fell for the ruse and provided the requested information, resulting in a compromise.

Report

To: accounting@securityscorecard.com

I need you to send me Most recent list of all unpaid vendors invoices or Aging Report .

Thank you

Aleksandr Yampolskiy

Chief Executive Officer

Securityscorecard

Image 1: Initial phishing email sent by adversary, appearing to be from SecurityScorecard's CEO.

Subsequent Attack

The threat actors used the information they obtained in the first attack to support a follow-up attack. They began by creating look-alike impostor domains for SecurityScorecard vendors, which were identified in the first attack. They then sent emails from these impostor domains asking SecurityScorecard recipients to update the banking details for the vendor to a CapitalOne account and pay outstanding invoices as soon as possible.

However, SecurityScorecard employees were skeptical and reported the incident, providing an excellent example of why employee training is key in these situations and why SecurityScorecard instills the importance of embodying “Security DNA” in its employees.

The threat actors conducted what is called a *business email compromise (BEC) campaign*, which is a social engineering attack that relies on people rather than technical sophistication. The motive behind these attacks are financial, usually attempting to convince a company to make payments to bank accounts under the actors control. A variation of a BEC campaign tends to see threat actors ask the victim to purchase prepaid gift cards and send pictures of the codes.

Striking Back

The response from SecurityScorecard's STRIKE team was swift and effective. The STRIKE team engaged in a counter-offensive operation to identify the threat actors' IP addresses and location.

First, STRIKE embedded a tracking pixel as a white, 1x1 pixel image in an emailed response from SecurityScorecard asking where the money should be sent. When the threat actor opened the email with images enabled, the tracking pixel sent the IP address and user agent stream back to collections infrastructure under STRIKE control.

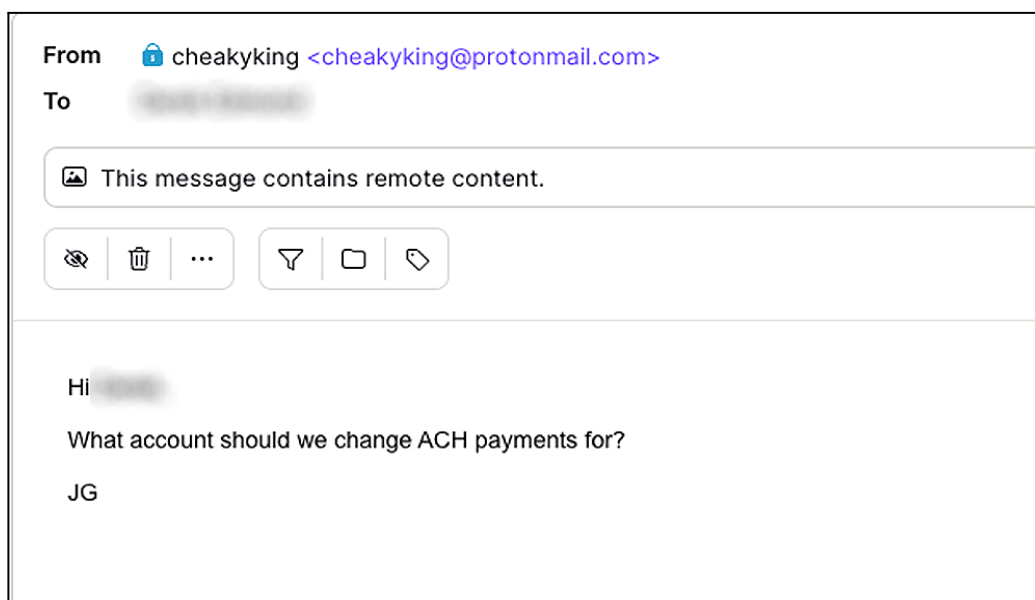


Image 2: Email to adversary asking for payment details.

The threat actors replied with the details of a CapitalOne account, which SecurityScorecard immediately reported to CapitalOne's Fraud Department, resulting in the account in question being frozen. SecurityScorecard believes that the CapitalOne account wasn't created directly by the threat actors. Instead, it was likely an account belonging to a money-mule, who is paid a commission on funds threat actors deposit and withdraw from the account. It appears that the attackers have a network of money-mules around the U.S that are used for such purposes.

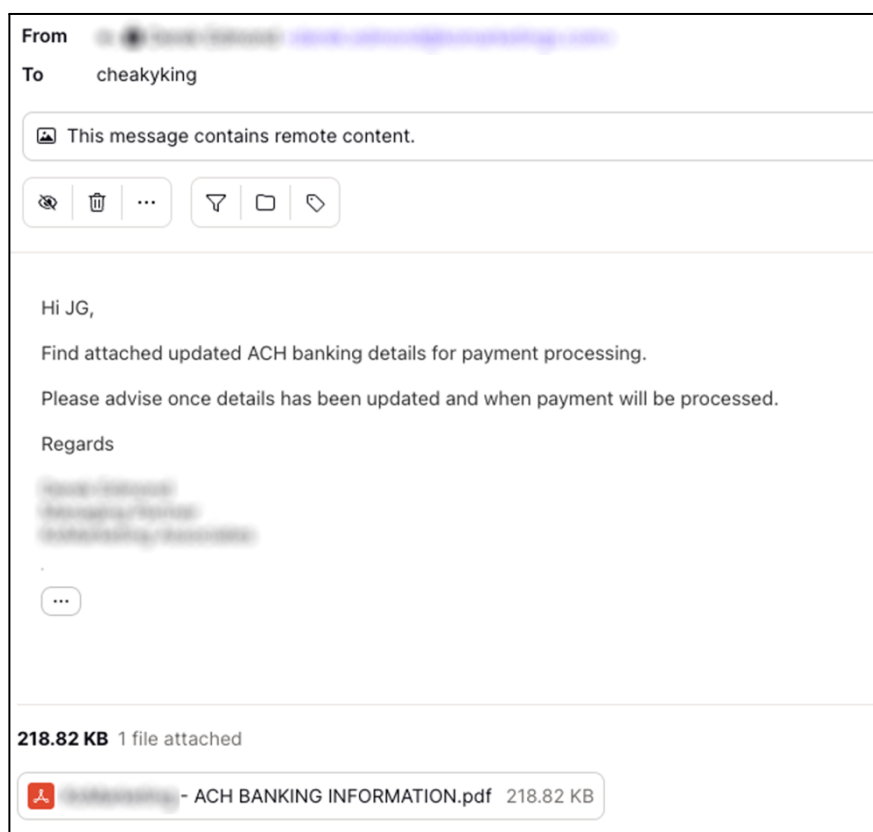


Image 3: Email from adversary impersonating vendor and requesting change to banking details.

Second, STRIKE embedded a link to a newly created honey-pot that mimicked a payment authorization gateway in a subsequent email to the threat actors. Using social engineering techniques, the email successfully lured the threat actors into clicking the link, exposing their actual location, a Remote Desktop Protocol (RDP) proxy server in India.

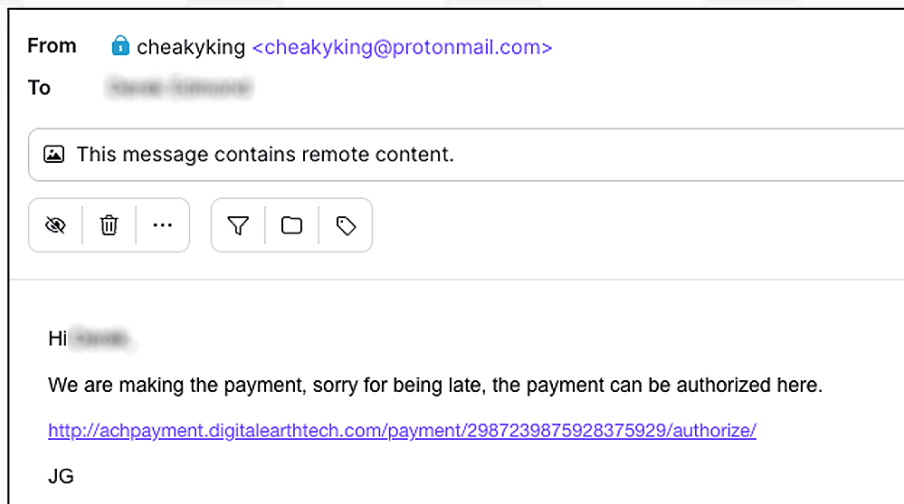


Image 4: Email to adversary with link to fake payment gateway.

Using Netflow analysis and other investigative techniques, STRIKE observed the threat actor using a sophisticated chain of VPN connections to connect to the India-based proxy server, from a location in Pakistan.

Since the counter-offensive operation, SecurityScorecard has had no further interaction with the threat actors.

Attributive Investigation Phases

The STRIKE team's actions were carried out in six phases:

Phase 1: Studying the Artifacts

Artifacts are tracks that a threat actor leaves behind. Analysis of artifacts allows investigators to find out more details about the incident and the adversaries's tactics, techniques and procedures (TTPs).

The main artifacts in this case are the emails and email addresses that were used to conduct the attack. By examining the headers contained in one of the spear phishing emails, STRIKE was able to identify the threat actor was accessing email from a Microsoft Azure IP (2.57.90[.]16), indicating that they were using Microsoft Office 365.

Phase 2: Correlating OSINT on the Attacker

After identifying the artifacts pertaining to the particular case, the next step was to correlate them with known open-source intelligence (OSINT) on the attacker. OSINT is a framework, but also a process for gathering and analyzing publicly available information for intelligence purposes. As such, it's a valuable tool for becoming more familiar with an attacker and their TTPs.

By looking at the OSINT available for this particular attacker, and enriching what was observed using SecurityScorecard's [Attack Surface Intelligence](#) (ASI), STRIKE discovered connections to a Middle East based Business Email Compromise (BEC) group that has been in operation since 2020. This group is known to use TTPs such as Spamming, SMTP takeover, domain impersonation, social engineering, invoice fraud, and obfuscation techniques including the use of VPN and RDP servers.

Our investigation uncovered that this was a sophisticated group that mainly targets large organizations. Three other organizations aside from SecurityScorecard were also targeted in the same manner within the same time-period.

A big part of OSINT is studying the reputational history of an attacker. SecurityScorecard analyzed the following indicators to determine the reputational history of this attacker:

- IP Address - Our team examined OSINT IP reputation feeds and determined that the IP address has a long history of abuse as it relates to invoice fraud and phishing.
- Domains - Passive DNS history on the IP address indicated an array of “imposter domains” that were tied to the IP address. An imposter domain is defined as a domain that impersonates a legitimate domain name registered by an attacker with the intent of using it for malicious purposes.

Phase 3: Investigating the Attack Origin Topology

The next stage of the investigation focuses on analyzing the infrastructure used to support the attack. Using tools such as SecurityScorecard's [Attack Surface Intelligence](#) (ASI) and Nmap scans, an investigator can learn more about the infrastructure used to support the attack.

By analyzing the infrastructure used to support this attack, STRIKE discovered that the attacker was most likely using a server that has a range of IP addresses aliased on virtual interfaces. This assumption is based on port scan results that indicate uniform responses across 2.57.90.0/24 on all ports, SSH hosted on port 65002 for the entire IP range with identical banners, and SSH authenticated with encryption certificates, not passwords.

```
$ telnet 2.57.91.5 65002
Trying 2.57.91.5...
Connected to 2.57.91.5.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.4

$ telnet 2.57.91.16 65002
Trying 2.57.91.16...
Connected to 2.57.91.16.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.4

$ telnet 2.57.91.96 65002
Trying 2.57.91.96...
Connected to 2.57.91.96.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.4
```

Image 5: Sample Nmap results for 2.57.90.0/24 IP range.

These findings indicated that the entire /24 range could possibly be used by the attackers, giving them the ability to operate on 255 different IP addresses. The large number of IP addresses allowed them to move to a different IP whenever one was negatively impacted by complaints or blacklists.

Phase 4: Investigating Attacker Origin

In any attack, threat researchers are motivated to attribute the attack to a specific group of threat actors, or at the very least, identify the probable location of the threat actors. Given the use of VPNs, Proxies, and relay-boxes, it can often be difficult to ascertain the true origin of an attack.

To overcome this challenge in this particular case, STRIKE utilized a honeypot server with a hyperlink designed to obtain the IP address of the adversary when clicked. An email was sent to the adversary instructing them to click the link which was mimicking a fake payment gateway. The adversary clicked the link, which unveiled two additional IP addresses used by the threat actor.

```
20.231.62.136 - - [04/Aug/2022 22:12:59] "GET /payment/2987239875928375929/authorize/ HTTP/1.1" 200 -
20.231.62.136 - - [04/Aug/2022 22:12:59] code 404, message File not found
20.231.62.136 - - [04/Aug/2022 22:12:59] "GET /favicon.ico HTTP/1.1" 404 -
20.219.186.247 - - [04/Aug/2022 22:14:31] code 404, message File not found
20.219.186.247 - - [04/Aug/2022 22:14:31] "GET /.env HTTP/1.1" 404 -
20.219.186.247 - - [04/Aug/2022 22:14:31] code 501, message Unsupported method ('POST')
20.219.186.247 - - [04/Aug/2022 22:14:31] "POST / HTTP/1.1" 501 -
```

Image 6: HTTP logs from honeypot server identifying adversary IP addresses 20.231.62[.]136 and 20.219.186[.]247.

Further analysis revealed that these two IP addresses were cloud-hosted Microsoft RDP servers located in India and the US. The actor likely first used 20.231.62[.]136 and when that attempt was unsuccessful they switched to 20.219.186[.]247 to attempt for a second time. This would explain why the attempts were two minutes apart.

```
$ echo | openssl s_client -connect 20.231.62.136:3389 | openssl x509 -text -noout
Can't use SSL_get_servername
depth=0 CN = hppc2
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = hppc2
verify error:num=21:unable to verify the first certificate
verify return:1
DONE
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      43:15:5e:95:62:3c:ef:b6:4f:9f:01:07:55:04:6e:d8
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN = hppc2
    Validity
      Not Before: Jul 24 17:48:20 2022 GMT
      Not After : Jan 23 17:48:20 2023 GMT
    Subject: CN = hppc2
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:db:c0:eb:49:bf:e3:04:ee:90:13:03:89:e1:dc:
        a5:aa:d0:7b:61:07:35:c6:15:c8:3f:f7:dd:71:56:
        9c:aa:5d:a6:39:9d:38:6a:6f:12:f4:c9:0c:55:46:
        16:ce:6f:07:68:92:58:8b:93:72:eb:fd:a2:60:4c:
        42:09:15:20:f0:a2:cb:77:bf:bb:b8:dc:b4:6f:3d:
        43:03:f3:72:e7:44:f8:6c:39:84:78:52:a6:4b:09:
        7f:7f:61:99:9d:e3:39:1a:07:a8:04:24:39:6f:02:
```

```

35:1f:b1:ab:14:9f:63:30:22:28:6f:8c:25:6d:38:
94:5a:5f:c4:d9:1a:ce:fa:e7:75:72:3e:0b:b0:d6:
7d:93:c7:0a:e9:77:2e:8f:33:6a:f8:6f:b7:07:af:
be:89:b0:9d:66:34:6d:03:cc:87:3e:8c:5c:3a:c5:
94:08:92:66:fa:fb:7d:11:29:ef:94:d8:87:30:f7:
ed:3c:01:bd:73:f8:d4:66:6e:be:2a:50:51:d2:1b:
11:d1:94:1f:ed:71:ee:02:46:19:fd:d4:c9:83:f8:
96:9f:69:30:65:a7:a7:83:e6:19:bc:fd:3d:9c:e1:
35:f3:60:bd:70:1b:aa:a1:d2:48:f4:e5:d3:ff:57:
ca:89:91:09:c4:1a:e2:43:9d:28:84:1d:35:9c:c7:
96:f1
    Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Extended Key Usage:
        TLS Web Server Authentication
    X509v3 Key Usage:
        Key Encipherment, Data Encipherment
Signature Algorithm: sha256WithRSAEncryption
88:7c:58:2a:20:2b:4e:ab:e6:da:e2:f7:7a:30:9a:93:4c:08:
9e:54:78:c5:b7:48:08:91:7d:bb:0d:f3:5d:d3:3f:6c:94:e8:
57:0a:76:e9:af:7f:58:58:3f:20:4d:a1:04:c4:89:ee:6f:a1:
5b:e4:ad:33:79:eb:b6:3e:40:11:b9:0e:bf:cd:1b:c5:67:7d:
45:87:07:13:b3:05:c0:8c:03:19:d6:a8:17:dc:2b:f2:89:f4:
76:40:f8:7f:b3:38:e5:81:c4:13:6a:29:43:93:dd:1e:a1:65:
60:7a:c6:51:a9:d3:28:4f:06:7c:bf:34:10:9b:ea:eb:7d:ae:
86:d2:75:e9:5a:c2:b0:53:85:ad:2a:3a:a3:80:d3:e9:f5:89:
09:2a:b7:1d:4c:b7:b4:dc:81:86:ef:11:27:b7:73:0d:84:63:
81:45:2f:b3:ff:63:f4:fc:13:fe:19:8d:bc:0c:e2:67:f2:b0:
7d:42:f4:f5:18:09:7b:88:97:67:17:fb:ae:c2:c3:4c:67:37:
e4:01:6b:38:36:22:9a:ae:a8:88:68:c3:a1:83:f3:93:61:c9:
31:02:45:fa:fd:1c:be:ce:89:75:3e:b6:59:3a:5f:56:03:e8:
e1:93:52:24:10:84:bd:f9:a6:55:3b:59:c4:91:46:ad:b2:49:
29:45:de:8a

```

Image 7: SSL Certificate on RDP port 3389 of 20.231.62.[.]136

```

$ echo | openssl s_client -connect 20.219.186.247:3389 | openssl x509 -text -noout
Can't use SSL_get_servername
depth=0 CN = caolan
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = caolan
verify error:num=21:unable to verify the first certificate
verify return:1
DONE
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      53:4b:fe:73:9b:84:7d:99:4d:2a:94:3c:d7:03:61:3a
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN = caolan
    Validity
      Not Before: Jul 30 14:03:42 2022 GMT
      Not After : Jan 29 14:03:42 2023 GMT
    Subject: CN = caolan
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:a8:05:8c:bf:5a:30:12:e8:b0:cb:b3:00:e7:47:
        57:21:e3:44:f8:b2:2b:1d:a2:84:d4:e2:52:7a:de:
        b0:ed:26:be:c0:52:79:52:0a:dd:61:bc:6b:c9:e0:
        7a:97:04:d7:b9:77:63:ba:fe:3c:ec:5b:f4:92:ea:
        d2:e5:52:de:ab:33:a8:17:68:0b:1c:17:d3:4f:6f:
        1c:87:b4:54:f7:a1:9c:f6:db:63:ae:b6:11:88:e1:

```



```

42:dd:36:da:4a:8e:62:70:df:21:76:5e:c1:14:2a:
90:6b:54:22:4e:8d:a8:e8:cb:02:e6:9e:f3:00:4f:
30:4c:57:d7:a2:96:46:3e:95:81:1e:27:5e:85:b0:
5a:e3:65:fc:e7:36:71:34:b2:fb:fe:3c:4c:d0:df:
cb:f5:6c:05:06:7a:ac:44:22:0e:f6:76:5e:68:a2:
64:a7:7f:ed:b2:99:d6:64:1c:69:87:67:63:65:91:
d1:33:32:ac:41:8e:f4:94:b6:ff:5d:df:23:3b:6f:
9f:aa:1b:93:2d:fd:fb:55:81:6b:b2:92:42:42:52:
7b:8e:70:28:e5:f1:9b:6a:e3:0d:e9:ae:e4:a4:af:
d7:91:cd:06:f3:17:d0:75:a5:98:54:c4:78:27:cf:
72:0d:11:5c:9f:d1:c6:81:f0:76:17:dd:58:28:ab:
26:dd
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Extended Key Usage:
  TLS Web Server Authentication
X509v3 Key Usage:
  Key Encipherment, Data Encipherment
Signature Algorithm: sha256WithRSAEncryption
27:94:11:08:c9:1a:ff:33:a0:b6:2a:e5:4b:7b:79:8d:fc:03:
53:6c:80:30:86:33:6e:1a:55:31:b5:1a:b9:b6:47:c8:d3:8d:
20:81:bc:e3:52:39:8c:e1:7c:7e:8f:20:68:29:4e:86:9c:31:
77:17:64:da:f0:0d:a7:89:c6:ba:18:bf:f8:a3:7c:ca:a4:06:
94:0d:a6:24:ec:ed:af:32:9d:65:32:1d:07:9b:a0:c8:c7:40:
d9:49:7b:66:b8:88:87:04:97:8f:16:d4:12:24:94:1c:b9:22:
f3:bf:2c:d8:04:7b:e3:73:f0:bf:42:e7:6e:44:bc:08:be:eb:
c4:72:81:05:87:92:71:82:e1:4a:78:45:99:80:91:7c:ca:ec:
e3:e1:c1:74:9a:b8:d6:ca:fa:a2:66:00:88:f1:47:43:6a:3a:
63:2c:32:8b:8f:1c:48:88:80:f1:c9:e6:46:ca:c5:bf:6b:2f:
b9:23:f4:90:a4:c7:6e:99:53:52:76:e5:3c:98:a1:52:3e:8a:
b5:a5:62:c7:07:f6:41:c5:bf:87:09:bc:60:cf:5f:7c:fc:3e:
35:bf:0d:85:02:38:9f:f8:fa:18:6d:55:6a:59:d2:6f:04:b1:
0e:75:d6:8d:98:94:04:eb:7b:24:3a:42:42:7a:05:9b:4b:48:
95:62:c9:55

```

Image 8: SSL Certificate on RDP port 3389 of 20.219.186[.]247

Given that the IP addresses obtained during the honey-pot operation were that of Microsoft RDP servers and not that of the attacker themselves, STRIKE needed to go one step further in its investigation. STRIKE analyzed netflow from the two IP addresses, 20.231.62[.]136 and 20.129.186[.]247, during the same time they were seen interacting with the honey-pot. What STRIKE observed was that shortly before this interaction, IP addresses from the 2.57.90[.]24 had two-way sessions with IP 20.129.186[.]247.

The IP addresses identified by the honeypot server were observed communicating with the /24 IP address range of the attacking server shortly before the attack was launched.













Start Time	Src IP	Dest IP	Proto	Src Port	Dest Port
2022-08-02 07:48:16	20.219.186.247 [info] 	2.57.91.209 [info] 	6 (TCP)	59883	443 (https)
2022-08-02 08:01:09	20.219.186.247 [info] 	2.57.91.209 [info] 	6 (TCP)	54839	443 (https)
2022-08-02 08:19:41	2.57.91.209 [info] 	20.219.186.247 [info] 	6 (TCP)	443 (https)	57733
2022-08-02 08:22:21	2.57.91.153 [info] 	20.219.186.247 [info] 	6 (TCP)	80 (http)	55448
2022-08-02 08:29:05	2.57.91.209 [info] 	20.219.186.247 [info] 	6 (TCP)	443 (https)	54824
2022-08-02 08:29:06	2.57.91.209 [info] 	20.219.186.247 [info] 	6 (TCP)	443 (https)	52282

Image 9: Netflow analysis of IPs

Netflow analysis revealed connections to the RDP box originating dynamic residential IP addresses located in:

- Pakistan
- Kenya
- South Africa

Phase 5: Reporting Attacks & Initiating Takedowns

The final phase of the investigation consists of summarizing and documenting findings, recommending solutions to ensure this type of breach doesn't happen again, and reporting to relevant authorities, partners, vendors, etc.

SecurityScorecard shared what it found with law enforcement agencies and service providers encountered during the investigation to initiate takedowns and other repercussions.

How SecurityScorecard can Help You With a Similar Investigation

SecurityScorecard is the global leader in cybersecurity ratings, trusted by over 30,000 organizations globally for actionable security data at every step of the cybersecurity lifecycle. SecurityScorecard offers the most holistic ratings platform, with an outside-in view of risk and inside-out view of risk; meaningful cyber risk reporting; professional services to build strong defenses and respond to any incident; and a marketplace of apps and integrations to integrate to your existing tech stack. During this investigation, the STRIKE team leveraged the following SecurityScorecard products and services:

Cyber Risk Intelligence (CRI) is an intelligence service delivered by the STRIKE team that combines expert-led, human analysis with deep and dark intelligence sources to deliver customized, actionable reports to meet the needs of an organization. CRI includes two service offerings: Core service reports including leaked credentials, imposter domains, hacker chatter, and APT reconnaissance and custom investigation reports to meet an organization's specific cyber security and threat intelligence needs, including deep dive research, malicious email analysis, leaked data and code discovery, malware analysis, and more. To learn how CRI can help your organization, [contact our STRIKE team](#).

Attack Surface Intelligence (ASI) is a threat and risk intelligence tool that brings together deep and relevant global data to help you identify and prioritize critical and non-critical threats for faster, more efficient risk mitigation. With SecurityScorecard's Attack Surface Intelligence (ASI), threat hunters and cybersecurity professionals can now effectively understand what the adversary's next step is before it causes disruption. All of this intelligence displayed in one platform enriches business decisions and empowers your team to take action in the right direction. See ASI in action and [get started for free today](#).

About STRIKE Team

SecurityScorecard's Threat, Research, Intelligence, Knowledge and Engagement (STRIKE) team is an elite team of cyber security experts with over 100 years of collective experience in cyber security investigations and research. STRIKE Team members come from varying backgrounds, including experience with intelligence services, special operations units, and Fortune 50 cyber threat intelligence teams.

About SecurityScorecard

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, with more than 12 million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 30,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity rating company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base. SecurityScorecard continues to make the world safer by transforming how companies understand, improve and communicate cybersecurity risks to their boards, employees, and vendors. Every organization has the universal right to its trusted and transparent [Instant SecurityScorecard rating](#). For more information, visit securityscorecard.com or connect with us on [LinkedIn](#).