Malwarebytes LABS

PRESENTS

Cybercrime tactics and techniques

Q2 2020

Table of contents

Attack on home base

The coronavirus pandemic has left the world looking very different at the end of the quarter than it did at the beginning. For starters, millions of workers are out of the office and working from their homes. This change in scenery, combined with safe social distancing efforts that help prevent the spread of COVID-19, has created a crisis for many, but an opportunity for some.

Employees are accessing company resources through VPNs, utilizing cloud-based services, and spending countless hours chatting on communication tools, all while connecting through personal networks and machines. In response, cybercriminals have been deploying campaigns to trick users into installing malware that steals login information for these sites, as well as provide remote control of the endpoint to the attacker.

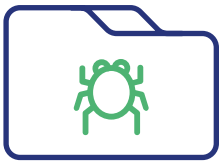
This special, COVID-19 themed CTNT report for January 2020 to March 2020 looks at the most prominently spread malware families taking advantage of this crisis, as well as other cybercriminal efforts we observed. We will give you a look into what the campaigns that spread these threats look like and the capabilities of the malware, along with information about card skimmers and APT attacks, wrapping up with some tips on staying safe.

Distributed malware

Threats like Emotet and Trickbot are still a big concern for businesses all over the world, however, the threats we are going to cover in this section are specifically using COVID-19 themed campaigns to spread. In fact, many of the families we have seen being installed by these campaigns have had very little success prior to the last few months. These changes represent a shift by cybercriminals to focus on a new target, your home base.

> **The threats we are going to cover in this section are specifically using COVID-19 themed campaigns to spread.**

AveMaria



Malware profile

AveMaria is a Remote Access Trojan used for taking over the systems of its victims and providing the attackers with remote control capability. It was first observed being spread through malicious phishing campaigns in 2018 and its presence on infected endpoints has been on the rise ever since.

Detection name:

Backdoor.AveMaria.*
Trojan.AveMaria
Spyware.AveMaria

First seen:

December 2018

Category:

Remote access trojan

Capabilities:

- Remote desktop access
- Remote webcam control
- Password stealer
- Downloader
- Keylogger
- Remote shell
- Privilege escalation

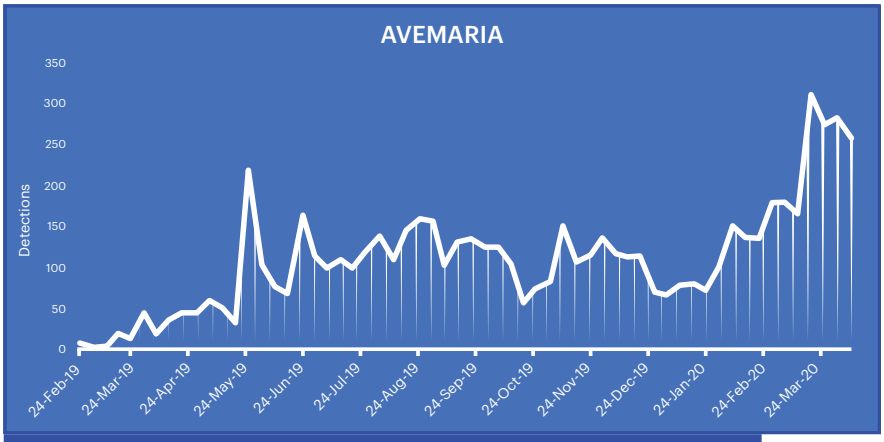


Figure 1. AveMaria detections, February 2019 - March 2020

Recent activity:

The AveMaria Remote Access Trojan is available for cybercriminals to purchase on the dark web for **about $23 for a monthly "subscription."** Over the last three months, we have seen an increase in detections of this threat, with a 109.6 percent increase between February and March.

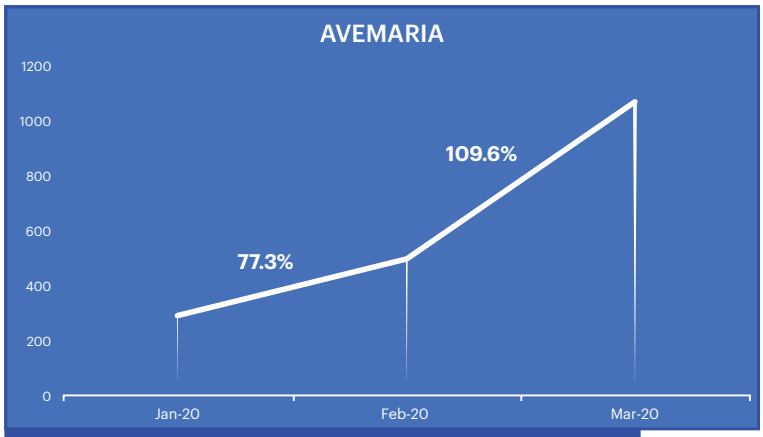


Figure 2. Avemaria percentage change January - March 2020

Spread via:

AveMaria has been observed recently being **spread through malicious phishing emails** claiming to contain information about effective face masks as well as through other COVID-19 themed campaigns.

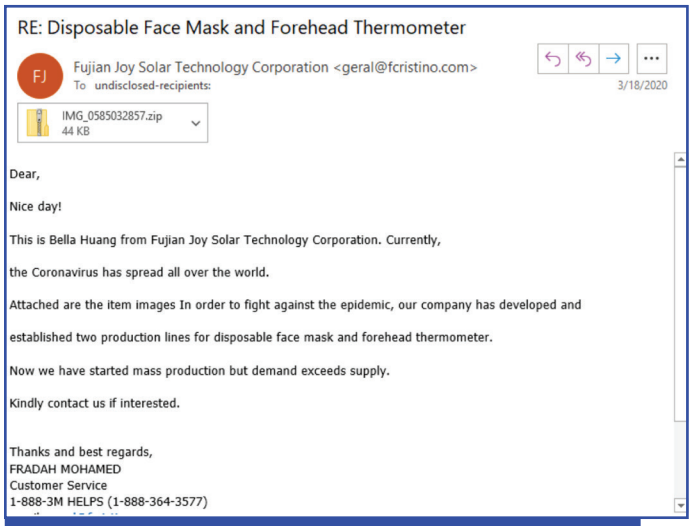
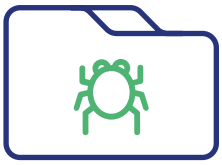


Figure 3. COVID-19 themed phishing campaign spreading AveMaria

NetWiredRC



Malware profile

The backdoor NetWiredRC has been associated with numerous types of attacks and threat groups, including the state sponsored group **APT33—Iranian-sponsored hackers with a focus on energy industries,** since its discovery in 2014. This malware is incredibly capable and dangerous, armed with the ability to manipulate, spy on, and steal data and applications from the user.

Detection name:

Backdoor.NetWiredRC.*

First seen:

November 2014

Category:

Backdoor access

Capabilities:

- Downloader
- Keylogger
- Information stealing
- System manipulation
- Provide remote access

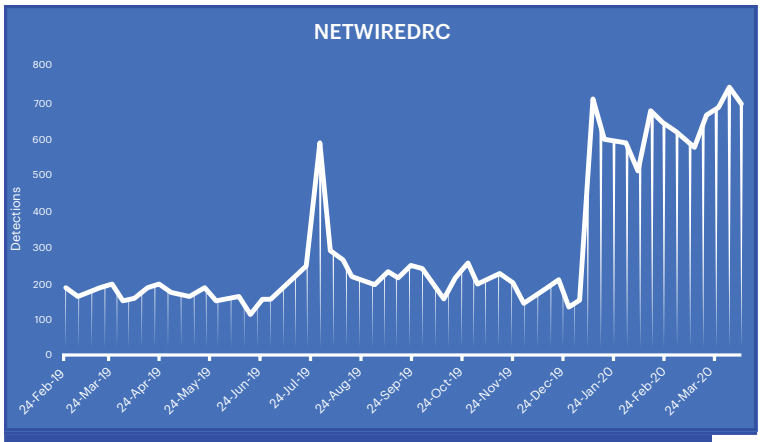


Figure 4. NetWiredRC detections, February 2019 - March 2020

Recent activity:

We have observed a roughly 40 percent increase in NetWiredRC detections since the beginning of the year. During the summer of 2019, NetWiredRC was involved with a phishing campaign **targeting the hotel industry in North America.**

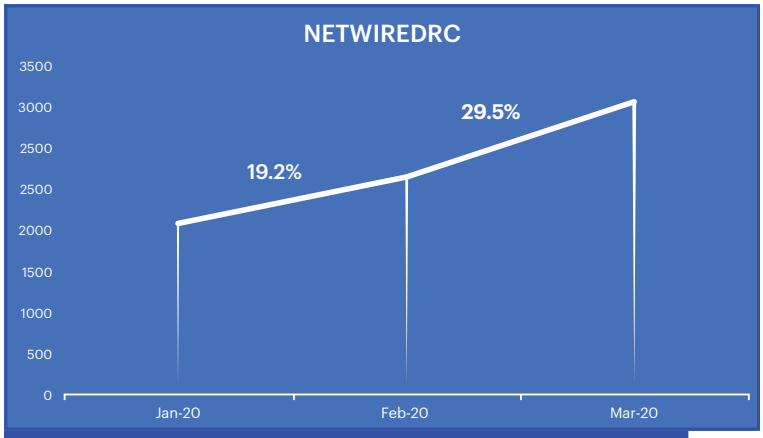


Figure 5. NetWiredRC percentage change January - March 2020

Spread via:

This malware has been observed primarily through malicious phishing campaigns, using numerous themes and ploys to get users to install the malware. A recent campaign claimed to be providing COVID-19 information from UNICEF, the children's aid organization.

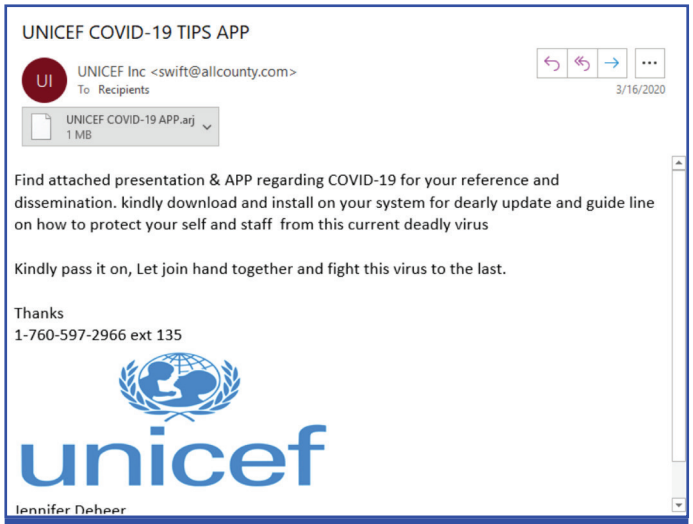
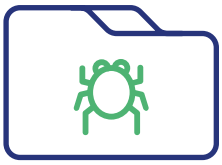


Figure 6. Phishing email impersonating UNICEF, spreading NetWiredRC

LokiBot



Malware profile

LokiBot is a well-known botnet which has been active since 2015. Its primary method of spreading has been through malicious emails or as a secondary payload for other downloader malware families. It is also known to use **stenography to hide malicious code** inside images.

Detection name:

Backdoor.Lokibot.*
Spyware.Lokibot.*
Trojan.Lokibot.*

First seen:

2015

Category:

Botnet, Information seeker

Capabilities:

- Keylogger
- Password stealer

Recent activity:

In addition to impersonating banks and shipping companies, LokiBot has been seen by multiple security research groups as a possible payload for many of the COVID-19 themed phishing campaigns that are active today. During the coronavirus pandemic, we have seen a 61.8 percent rise in LokiBot detections.

Spread via:

LokiBot is most notably spread through malicious phishing campaigns. Recently, we've observed this malware being pushed as an invoice for a medical supply pusher.

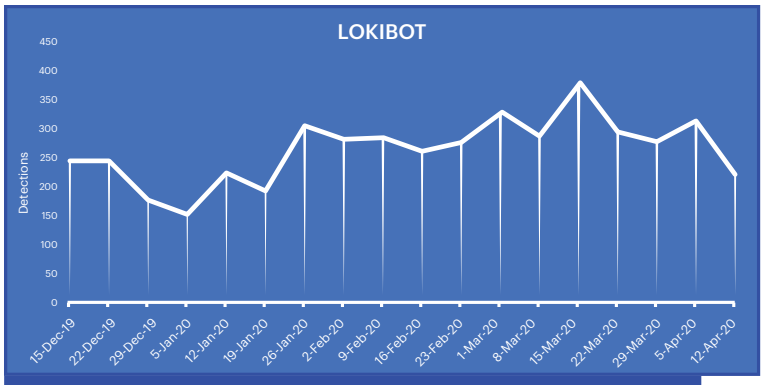


Figure 4. LokiBot detections, December 2019 - April 2020

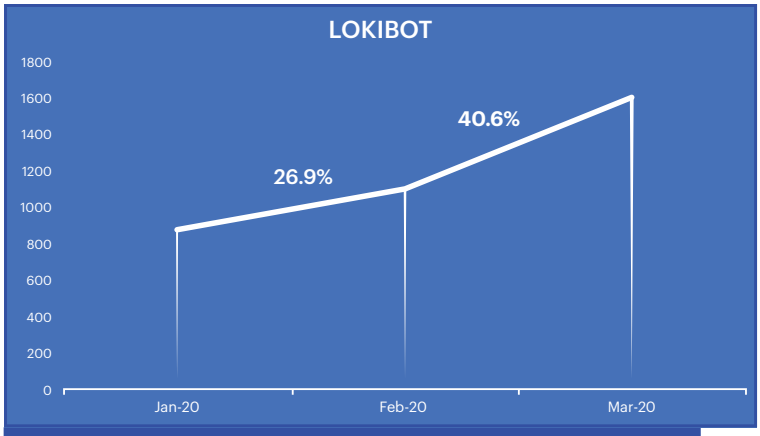
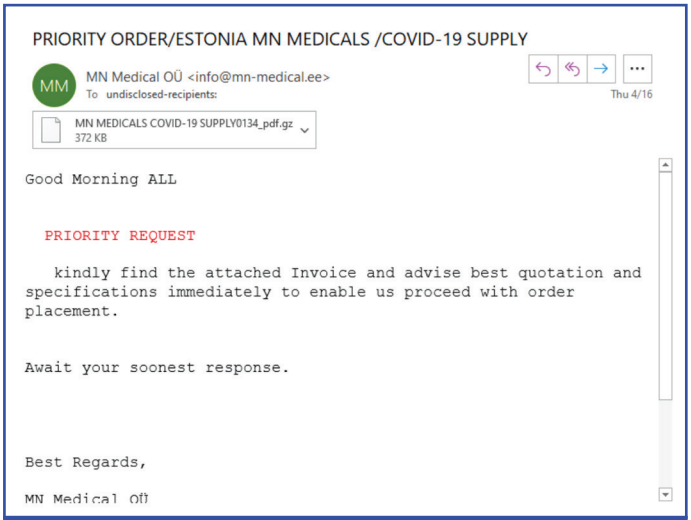


Figure 8. LokiBot percentage change January - March 2020


PRIORITY ORDER/ESTONIA MN MEDICALS /COVID-19 SUPPLY

MM

MN Medical OÜ <info@mn-medical.ee>
To undisclosed-recipients:

Thu 4/16

MN MEDICALS COVID-19 SUPPLY0134_pdf.gz
372 KB

Good Morning ALL

PRIORITY REQUEST

kindly find the attached Invoice and advise best quotation and specifications immediately to enable us proceed with order placement.

Await your soonest response.

Best Regards,

MN Medical OÜ

Figure 9. COVID-19 themed phishing campaign pushing LokiBot

AZORult

Malware profile

AZORult is a **dangerous information stealing malware that has been on the scene since 2016.** This malware can also act as a downloader for other malware and has previously been installed as a secondary payload to families like Emotet. The primary method of infection for this threat is through malicious phishing campaigns and drive-by exploits.

Detection name:

Backdoor.AZORult.*
Spyware.AZORult.*

First seen:

July 2016

Category:

Information stealer

Capabilities:

- Password stealer
- Cryptocurrency theft
- Downloader

Recent activity:

The AZORult malware remained a steady threat throughout 2019. Then, starting in November, we began to see a larger increase in detections until around February. However, a comparison with March shows a 30.1 percent increase in detections of this threat, month over month, proving that this threat is **likely not going away soon.**

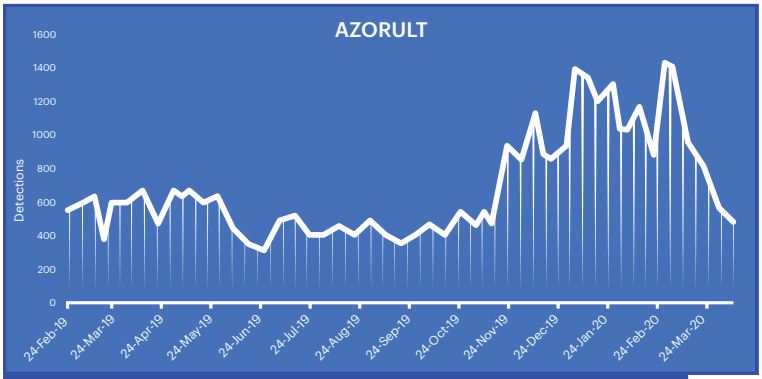


Figure 10. AZORult detections, February 2019 - March 2020

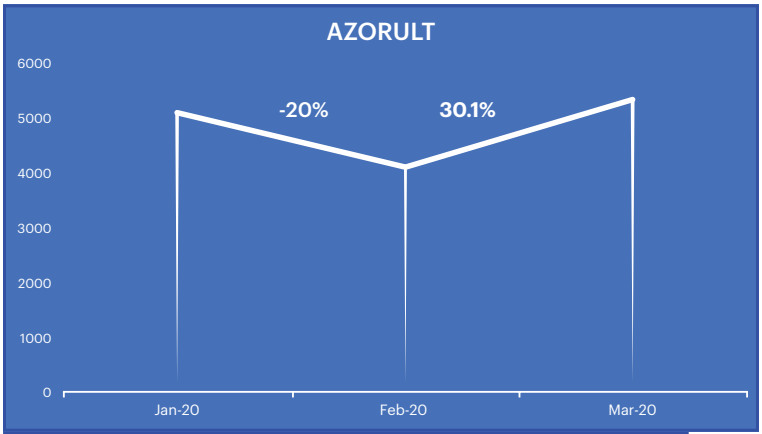
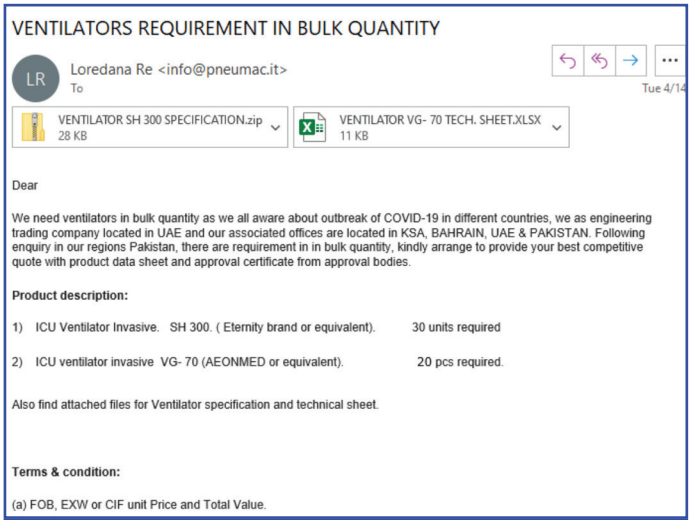


Figure 11. AZORult percentage change January - March 2020

Spread via:

AZORult has been observed recently as a possible payload for numerous COVID-19 themed attacks, including one asking the recipient for bulk quantities of ventilators as well as being one of the payloads attached to [a fake Johns Hopkins University coronavirus map application.]


VENTILATORS REQUIREMENT IN BULK QUANTITY

LR Loredana Re <info@pneumac.it>
To
Tue 4/14

VENTILATOR SH 300 SPECIFICATION.zip 28 KB
VENTILATOR VG- 70 TECH. SHEET.XLSX 11 KB

Dear

We need ventilators in bulk quantity as we all aware about outbreak of COVID-19 in different countries, we as engineering trading company located in UAE and our associated offices are located in KSA, BAHRAIN, UAE & PAKISTAN. Following enquiry in our regions Pakistan, there are requirement in in bulk quantity, kindly arrange to provide your best competitive quote with product data sheet and approval certificate from approval bodies.

Product description:

1) ICU Ventilator Invasive. SH 300. (Eternity brand or equivalent). 30 units required

2) ICU ventilator invasive VG- 70 (AEONMED or equivalent). 20 pcs required.

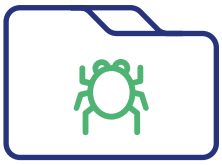
Also find attached files for Ventilator specification and technical sheet.

Terms & condition:

(a) FOB, EXW or CIF unit Price and Total Value.

Figure 12. COVID-19 themed phishing campaign pushing AZORult

DanaBot



Malware profile

DanaBot is a family of banking trojan malware, first discovered being distributed by malicious emails, with a focus in Australia. It has recently been distributed through malicious advertisements using the RIG & Fallout exploit kits. However, DanaBot's spread has expanded as of late, as infections have been spotted in various countries in Europe as well as North America.

Detection name:

Backdoor.DanaBot
Spyware.DanaBot
Trojan.DanaBot

First seen:

May 2018

Category:

Banker trojan,
Information stealer

Capabilities:

- Bank credential theft
- Password stealer
- Downloader
- Browser manipulation
- Phishing website redirection

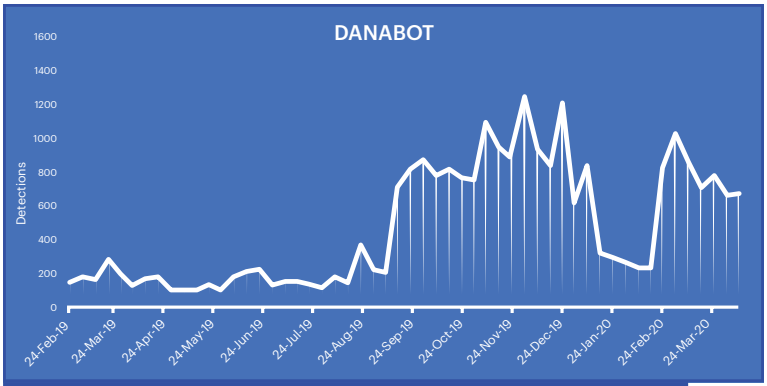


Figure 13. DanaBot detections, February 2019 - March 2020

Recent activity:

DanaBot has been active since September of 2019, with a dip in detections between January and February 2020. This dip resulted in a rise of 166 percent in detections between February and March 2020.

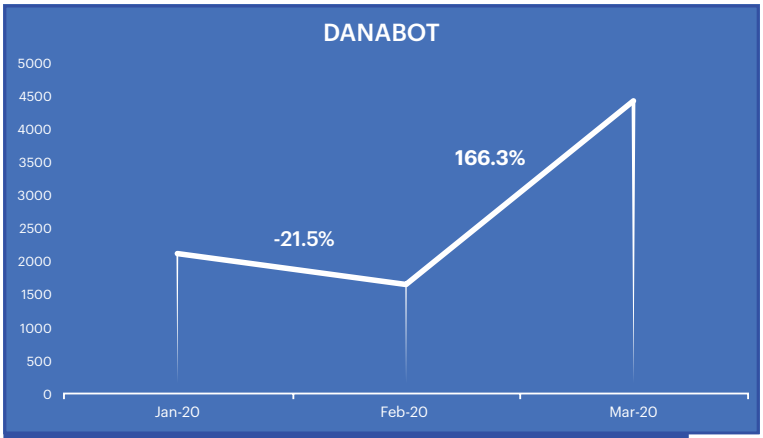


Figure 14. DanaBot percentage change January - March 2020

Spread via:

DanaBot is being spread in numerous ways, from exploit kit malvertising attacks, to malicious email campaigns. The Polish CERT organization **recently sent a warning to Polish citizens** about a campaign pushing the DanaBot malware through malicious PowerPoint presentations. In addition, DanaBot is one of the possible payloads we may see installed by the fake **Johns Hopkins coronavirus map which was first discovered in March.**

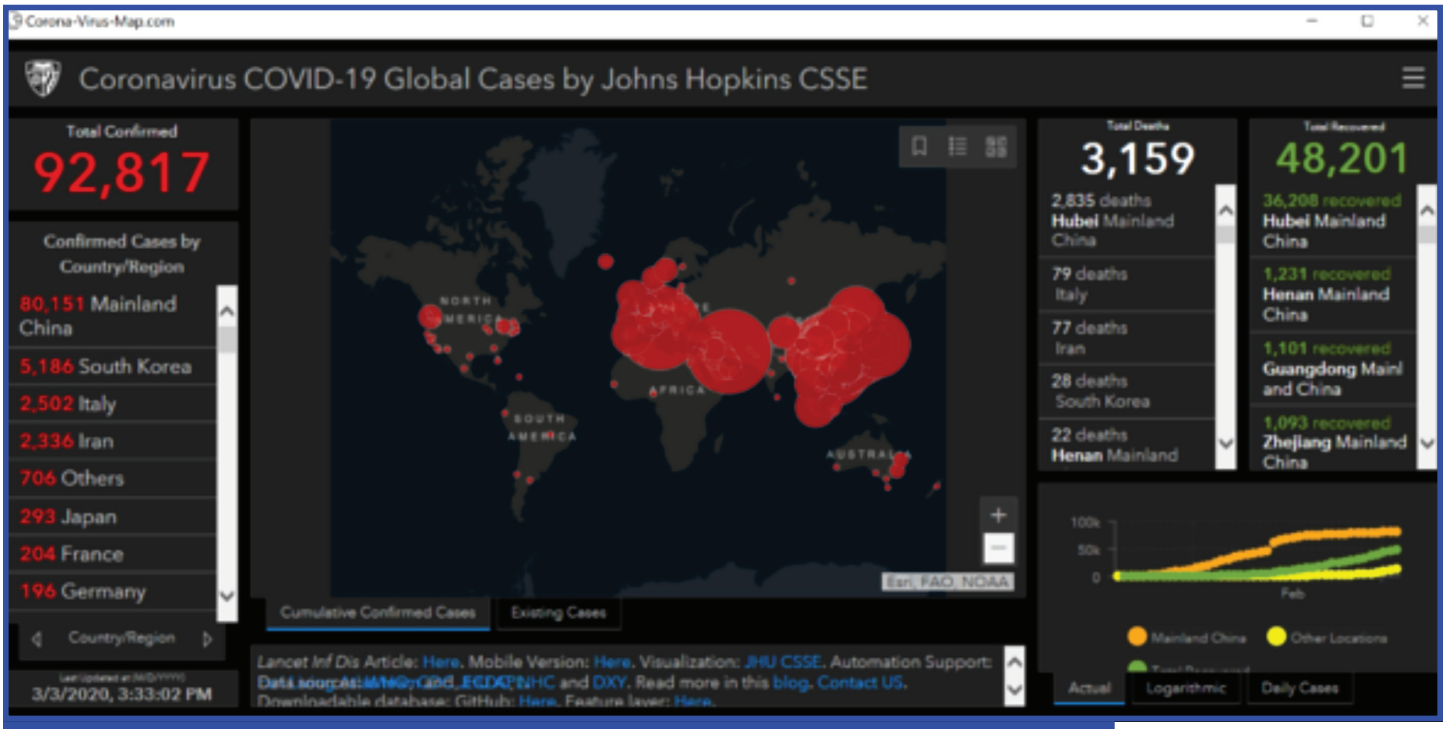


Figure 15. Fake Johns Hopkins University coronavirus map application used to spread malware like DanaBot

Other efforts

Phishing emails and scary maps are not the only criminal operation we have seen taking advantage of the current state of the world. In fact, home shoppers are at a greater risk than ever with an increase in credit card skimmers found on webstore checkout pages. In addition, government sponsored actors are trying to blend their attacks in with the flood of coronavirus themed scams.

Card skimmers:

Panic buying, hoarding, and a drastic change in how we purchase goods—from in-store to delivery and pickup—has resulted in rushed deployments of online order forms, price manipulation, counterfeit goods and, of course, online scams. Cybercriminals focused on stealing financial data from users have **increased the compromise of online order forms and installation of card skimming code** on these web pages. We have seen a 26 percent increase in this kind of attack from February to March 2020.

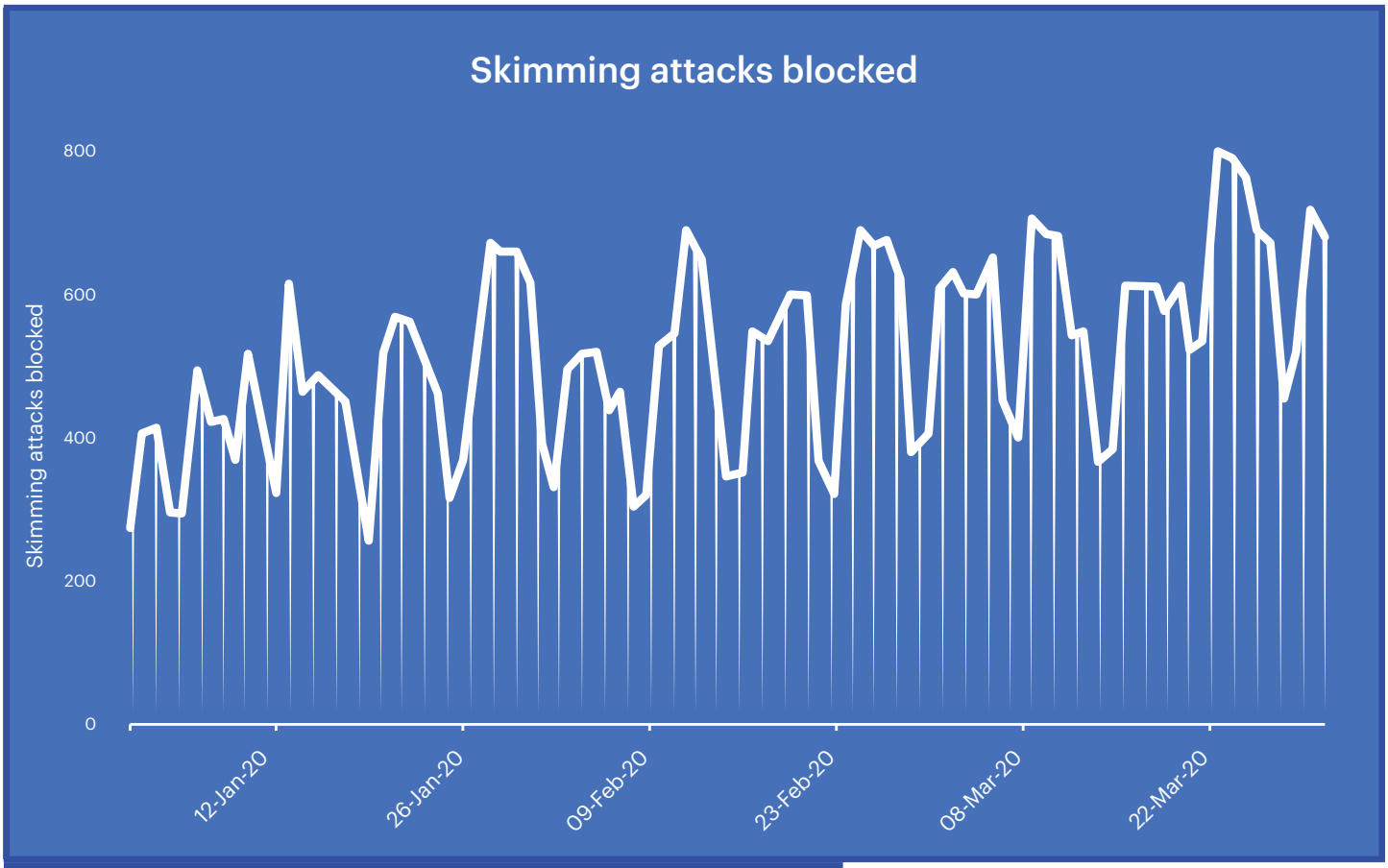


Figure 16. Increase in card skimmer URLs blocked, January – March 2020

You can find out more about the rise in card skimmers and about some notable companies whose customers have become victims of this method of attack on the Malwarebytes Labs blog: **"Online credit card skimming increased by 26 percent in March."**

State sponsored attacks:

Using COVID-19 as bait to trick users is not solely a trick of the commercial cybercriminal; in fact, numerous state-sponsored groups have used this theme in phishing attacks against relevant targets.

From late January on, several cybercriminal and state-sponsored advanced persistent threat (APT) groups have been using coronavirus-based phishing as their infection vector to gain a foothold on victim machines and launch malware attacks. Just like the spread of coronavirus itself, China was first hit by APT groups and as the virus spread worldwide, so did the attacks.

Their method of spreading threats with emails varies depending on the group—some use template injections, others use RTF exploits, and the majority use malicious macro scripts, like the modus operandi of non-state-funded attackers.

To read more about state-sponsored actors using COVID-19 as bait, check out the Malwarebytes Labs blog and a recent white paper we released: **"APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure."**

Protecting home base

The threat landscape of the last few months has been very different from the one we saw at the end of 2019. Attacks in the COVID-19 era are focused on stealing your information and using remote employees as doorways into more valuable networks. This means that we need to make sure to spread valuable security knowledge to protect people while they are working at home base.

Gain security through knowledge by:

1. Running security software on any system which is not only connected to your home network but is also used regularly. With this current flood of attacks, the malware families being deployed will change quickly to avoid detection and be difficult to defeat without updated security tools that monitor system applications and behavior.
2. Using a virtual private network or VPN. This will not keep you protected from malware; however, it will help to keep your online activities from your browser or connection revealing personal information or tracing your behavior. **This creates an additional measure of layered protection when you shop online.**
3. Using trusted sources for information, shopping, or applications. The spread of misinformation allows many of the attacks mentioned in this report to flourish. So, relying on certain trusted vendors, websites, and news sources is the best approach.
4. Avoiding repeated entries of credit card numbers into applications. Use something like PayPal, Apple Pay, Samsung Pay, or Google Pay, which can offer greater security of your financial information and reduce the chance that your card information will be spread online.
5. Changing online service passwords on a separate, trusted computer, then thoroughly cleaning the suspected system with an anti-malware application if there are identified active infections or suspected system or data compromise.

Conclusion

Themed phishing campaigns usually don't last too long. In fact, once enough information about their existence has been distributed, the attacks will become less effective and we'll see a return to regular attacks, like those pretending to be from a bank or shipping company. What is likely going to last is the capability of organizations to have their employees working remotely to cut down on overhead or as an alternative to working in an office. This reality also means that attackers who attempt to infiltrate organizations via their remote workers will continue to develop their tactics and techniques long into the future.

LABS | blog.malwarebytes.com corporate-sales@malwarebytes.com 1.800.520.2796