Orange
Cyberdefense

Security Intelligence | Research Report

Monthly Report August 23

8

www.orangecyberdefense.com

Contents

Introduction

VMware Aria SSH Bypass

CISA is urging users of VMware Aria Operations for Networks to immediately apply patches following the disclosure of a critical vulnerability in the network management tool. The vulnerability would allow a malicious actor with network access to Aria Operations for Networks to bypass SSH authentication to gain access to the Aria Operations for Networks Command Line Interface (CLI). The flaw is down to a lack of unique cryptographic key generation essentially resulting in "hardcoded" authentication keys.

Lockbit Leaks UK MoD Documents

Thousands of pages of UK MoD related documents have allegedly been leaked on the dark web by the prolific Cy-X group LockBit. The leak stems from a third-party supplier, Zaun, who manufacture fencing, and consists of 10GB of sensitive documents about sites such as His Majesty's Naval Base, Clyde (HMNB Clyde) nuclear submarine base, the Porton Down chemical weapon lab and GCHQ's communications complex in Bude, Cornwall.

The breach occurred when Zaun was hit by what they say was a "sophisticated" cyberattack on the 5th and 6th August, whereby a rogue Windows 7 PC running software for a manufacturing machine was accessed by LockBit allowing them to exfiltrate the data.

Zero-Day Bonanza

System and security admins have had their work cut out for them in recent weeks with the slew of actively exploited zero-day vulnerabilities being disclosed and patched. So far in September Apple, Microsoft, Google, Mozilla, Adobe, and Cisco have all had to urgently release advisories and patches.

The total number of zero-days seen from January thru August has been placed at around 60, with a further 10 already reported in September, with these values 2023 could easily be a record year for zero-days.

At a glance

Following the return from summer holidays it's now the time of year where members from several Orange Cyberdefense teams turn their focus and attention to this year's Security Navigator report.

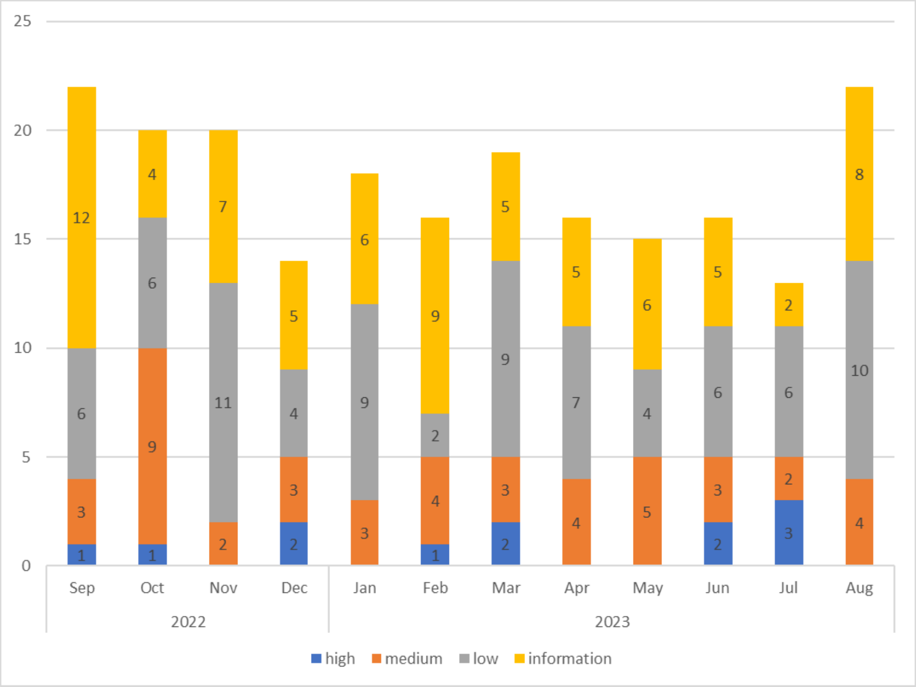
Following the success of last year's report, the pressure is on to try and surpass it and the launch date of 30 November will come around far too quickly!

If you haven't yet read the Navigator 2023, check it out here:

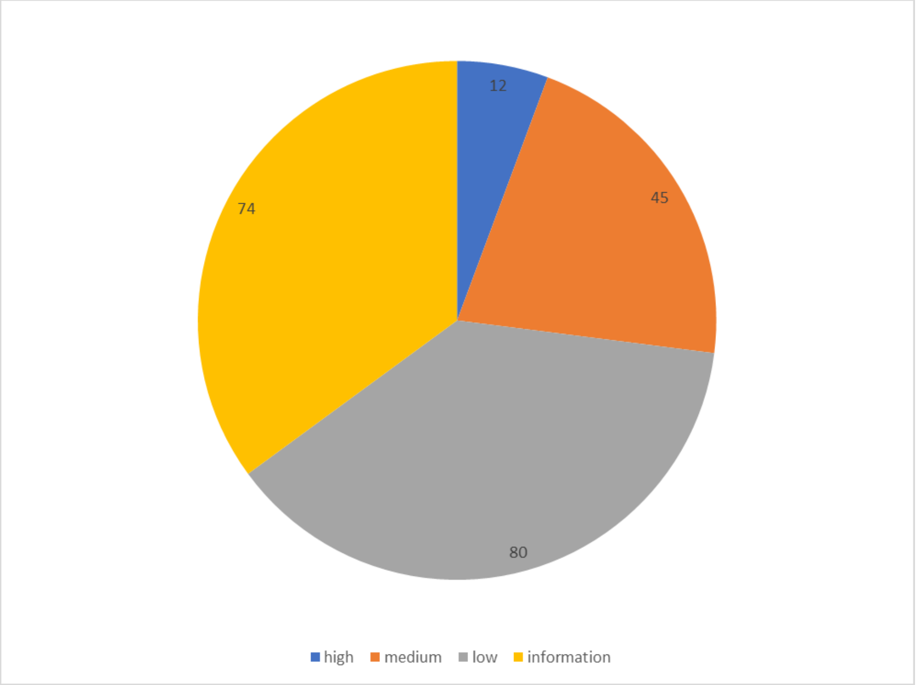
https://www.orangecyberdefense.com/global/security-navigator

World Watch Review

The Orange Cyberdefense CERT published a total of 22 new World Watch advisories during August 2023, along with adding updates to a further 19 previously published advisories.



Breakdown of Published Advisories Previous 12 Months

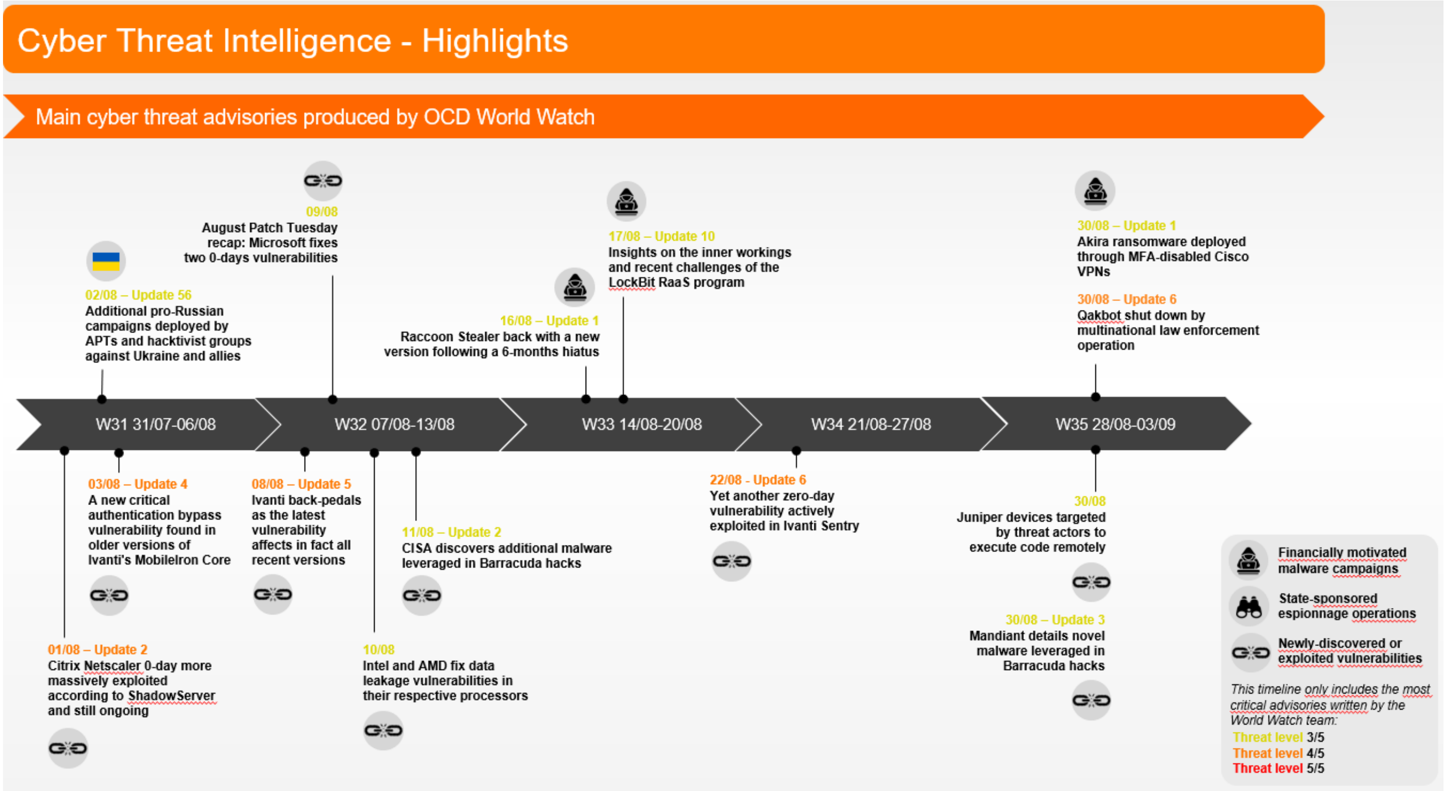


Breakdown of Advisory Criticality for Previous 12 Months

Advisory Summary

In August, as you can see in the first chart above, we had no advisories rated as high criticality, all advisories were given criticality ratings of medium, low or information when initially published. These ratings are based on our CERT's assessment of the risk and threat levels associated with the subject of the advisory at the time of publication, so even though an advisory may concern a vulnerability rated as critical by the vendor we may deem it to only initially be medium, if say there is no publicly available exploit. This is under constant monitoring however and subsequent updates will increase our criticality level as required if circumstances should change.

See below for a timeline of advisories rated Medium and higher:



Cyber Threat Intelligence - Highlights

Main cyber threat advisories produced by OCD World Watch

01/08 – Update 2
Citrix Netscaler 0-day more massively exploited according to ShadowServer and still ongoing

02/08 – Update 56
Additional pro-Russian campaigns deployed by APTs and hacktivist groups against Ukraine and allies

03/08 – Update 4
A new critical authentication bypass vulnerability found in older versions of Ivanti's MobileIron Core

08/08 – Update 5
Ivanti back-pedals as the latest vulnerability affects in fact all recent versions

09/08
August Patch Tuesday recap: Microsoft fixes two 0-days vulnerabilities

10/08
Intel and AMD fix data leakage vulnerabilities in their respective processors

11/08 – Update 2
CISA discovers additional malware leveraged in Barracuda hacks

16/08 – Update 1
Raccoon Stealer back with a new version following a 6-months hiatus

17/08 – Update 10
Insights on the inner workings and recent challenges of the LockBit RaaS program

22/08 - Update 6
Yet another zero-day vulnerability actively exploited in Ivanti Sentry

30/08 – Update 1
Akira ransomware deployed through MFA-disabled Cisco VPNs

30/08 – Update 6
Qakbot shut down by multinational law enforcement operation

30/08
Juniper devices targeted by threat actors to execute code remotely

30/08 – Update 3
Mandiant details novel malware leveraged in Barracuda hacks

Financially motivated malware campaigns

State-sponsored espionnage operations

Newly-discovered or exploited vulnerabilities

This timeline only includes the most critical advisories written by the World Watch team:

Threat level 3/5
Threat level 4/5
Threat level 5/5

Editor's Notes

Here the team will provide commentary on a news item, expansion on something specific such as a single incident, or could be as expansive as coverage on trends observed in the threat landscape.

Wicus

On life support?

I am willing to bet that the term "legacy system" is commonly spoken with a tone of disdain, followed by a sigh or even some gesture to ward off malicious exploitative spirits. Legacy systems are systems that remain operational longer than originally intended and normally have fallen behind with patches and as a result cannot be updated or changed due to a vendor or systems implementer that no longer supports the product. This concept of "End-Of-Life" (EOL) is also common in the IT and cyber security fraternity.

The OpenSSL team recently announced that it is ending public support for version 1.1.1 of the OpenSSL library in mid-September 2023. To the credit of the OpenSSL team, this version has been receiving free public security updates since 2018, or about 5 years. This sunsetting or EOL announcement is not supposed to be new information as the Long-Term Support (LTS) status of this particular version made it clear when the public support ends.
The reality is that version 1.1.1 of the OpenSSL library will most likely remain deployed on systems for some years to come. This is not wild speculation, but more an educated guess based on scanning data that our Vulnerability Operation Centers (VOC) have collected and the trends we have noticed.

Out of date or weak Secure Socket Layer (SSL) and Transport Security Layer (TLS) cryptographic configurations supported by unpatched OpenSSL libraries are commonly encountered in our scanning data set. Another group of findings we report on that seems to follow a similar pattern to weak SSL cryptographic configuration is associated with Secure Shell (SSH) services, specifically those associated with out-of-date OpenSSH versions.
The SSL/TLS vulnerabilities are normally found on web servers such as Apache HTTP and Apache Tomcat, but others such as Microsoft Internet Information Server (ISS) are also in the mix. Further reported unique findings also spill over into associated insecure web applications served by these dubious web servers that struggle with what are now considered basic web application security practices. Examples include the absence of explicit attributes related to protecting sensitive web cookies or forcing secure HTTP connections, etc.

The presence of weak cryptographic configuration relating to SSL/TLS is normally an indicator of an underlying weakness with the system, in other words unpatched or poorly maintained systems. This may be a gross generalization, but the theory we are testing is that if one component of the system is weak then that could point to other neglected parts of the system. In other words, if this kind of state is tolerated then what else is permitted to exist?

Looking at VOC data for the past year we find that 25 distinct organizations out of 41 organizations in our dataset, more than 60%, have findings where out of date SSL/TLS versions are present or running out of date OpenSSL libraries. Of these, 21 organizations have findings reported on assets labelled as “External”, implying that these assets have potentially greater exposure to threats that can originate from outside the borders of the organization. When considering assets labelled as “Internal” the number of organizations drops to 11. Seven organizations fall in either category, External or Internal. This means that 14 organizations in the result set only have assets labelled as External, while 4 organizations only have assets labelled as Internal.

How many assets or systems are impacted that are labelled as External or Internal only, and match our SSL search criteria? We find that 445 unique assets have been reported across the 21 organizations where assets are labelled as External. The picture is slightly different when looking at organizations with assets labelled Internal, with 2351 unique assets impacted by out-of-date SSL/TLS ciphers or weak cryptographic configuration. Assuming that “Internal” labelled assets are equivalent to systems that reside on the “inside” network behind traditional firewalls, then that means many unpatched systems are considered protected/mitigated by that association.

Are businesses then resigned to that fact as it’s easier to just accept the reduced risk and move on to more pressing matters, but what is that saying about not fixing broken windows? We will try to answer this question in the next Security Navigator that will be released at the end of November 2023.

Ric

Navigating the C(SIRT)

As with the rest of the Security Research Center team here at Orange Cyberdefense, I am right in the middle of working on this year’s Security Navigator. The specific area of our business I’m looking at telling the story for is the Cyber Security Incident Response Team (CSIRT). I don’t want to spoil too much of what will be discussed in the actual Security Navigator, so in this editorial I wanted to very briefly talk about the methodology that has gone into the CSIRT section and just a few narrative highlights that I’m excited to present.

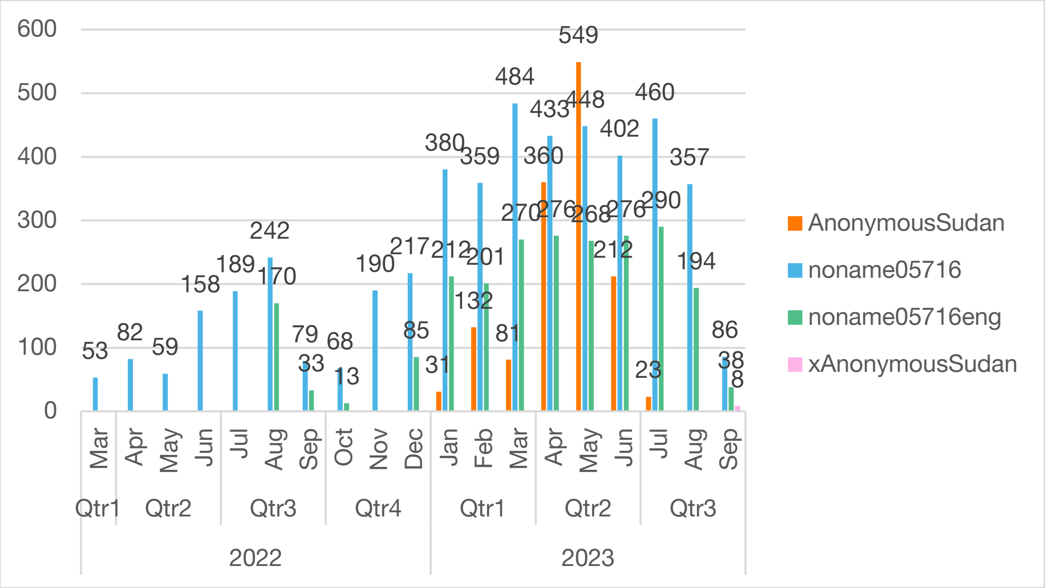
The collection for this year’s CSIRT data involved deep discussions with the leadership of both our CSIRTs to identify what their story is and how any data we collect fits in with the rest of the Security Navigator to also tell a cohesive story overall. What we quickly found was that, while we can extract interesting *explicit* information from the data such as indicators of compromise (IoCs), vulnerabilities exploited tracked by their CVE IDs, and victim demographics, there was much left unsaid. What was missing was that data's context, which only comes in the form of *tacit* information that is held solely in the knowledge gained through experience and practice of our CSIRTs. Therefore, to best tell our CSIRTs' stories, this year I am still collecting that quantitative, explicit data, but I am also conducting qualitative studies in the forms of interviews and surveys with our CSIRTs; this way, readers of the Security Navigator will not only understand 'what' our CSIRT data says but also 'so what', 'why', and 'how'.

Diana

Telegram bans hacktivist group's channel – hacktivist groups opens new channel within a day.

We are increasing our tracking capabilities to understand hacktivism with geopolitical implications better. After Russia began invading Ukraine in the beginning of February 2022; a surge in hacktivism began. Both sides, pro-Russian and pro-Ukraine, sought help from the cyber space. Two groups that have caught our particular interest are Anonymous Sudan and NoName0571, both use Telegram as a channel to communicate to the public.

Below we tested scraping activities from the respective Telegram channels. Here we count 'announcements' of each group. The announcements include a date stamp and the public announcement of an often-successful Distributed Denial of Service (DDoS) attack. July shows a small number because we scraped the data in the beginning of July 2023.



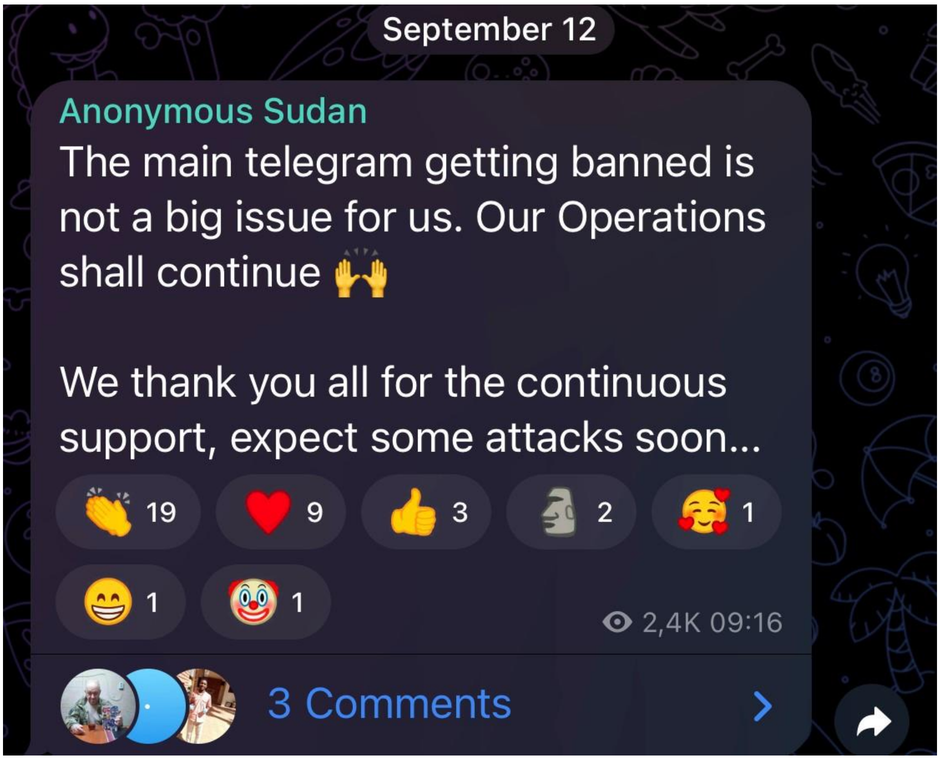
Hacktivist activity of Anonymous Sudan and NoName05716 over time

As can be seen above, NoName0571, who maintains one Russian speaking and one English speaking channel, has been active since the beginning of the war against Ukraine. Anonymous Sudan began their activities in January 2023. In total we scraped 2,669 announcements from all three channels between March 2022 and the beginning of July 2023.

Both groups have been impacting the Nordics, namely Denmark and Sweden quite extensively. While the goal and true origin of Anonymous Sudan is still controversial; NoName is a clear pro-Russian hacktivist group targeting institutions and countries that have shown commitments to provide aid to the Ukraine.

Telegram, a messaging platform, took action against Anonymous Sudan and suspended their main account on September 8th, 2023. At that time, Anonymous Sudan's channel had 120,000 subscribers. The hacktivist did not take the ban so well and began a DDoS attack on Telegram as retaliation. News coverage on this has been scarce, first English-speaking reports surfacing only a few days after[1,2].

While actions like this are necessary to combat illicit activities and abuse of platforms that were meant for legitimate usage, the case of Anonymous Sudan shows us that it took Anonymous Sudan only a day or less to just create a new channel. The new channel with the name @xAnonymousSudan was created on the 9th of September 2023. On the 12th of September, Anonymous Sudan posted the following statement:



September 12

Anonymous Sudan

The main telegram getting banned is not a big issue for us. Our Operations shall continue 🙌

We thank you all for the continuous support, expect some attacks soon...

[1] https://www.scmagazine.com/brief/telegram-targeted-by-anonymous-sudan-ddos-attack
[2] https://securityaffairs.com/150690/hacking/anonymous-sudan-ddos-on-telegram.html

Unfortunately, the ban did not have any effect on the hacktivist group’s activity. As they state themselves, ‘operations shall continue’. At the time of writing, the new channel has gained already more than 16K subscribers. This is a very good example of the challenges that providers such as Telegram face but also in a wider sense the challenges we as a society face.

Single, small-scale interruptions such as this one will not disrupt illicit activities in any meaningful way. What we need are more coordinated, collaborative, large-scale countermeasures that have the potential to disrupt these ecosystems. As we conclude our observation not just on hacktivism activities but also other forms of cyber aggressions: “One person’s/group’s takedown, is another’s opportunity.”

Good News Cyber

Duck Hunting Season

US officials claim to have permanently taken down and dismantled the notorious botnet known as Qakbot or Qbot. The international operation, which also involved law enforcement in France, Germany, the Netherlands, the United Kingdom, Romania and Latvia, 52 servers were seized along with more than $8.6 million in cryptocurrency.

Named "Duck Hunt", a play on the name of the botnet, the operation identified in excess of 700,000 infected computers globally. In order to dismantle the botnet authorities managed to gain access to the Qakbot network and subsequently the command-and-control servers, at which point traffic was redirected to FBI controlled servers. This then allowed FBI developed software to be sent to infected machines which, according to an FBI affidavit, "will untether them from the Qakbot botnet and prevent the Qakbot administrators from further communicating with the infected computers."

Fake Call Centre Raided

Polica in Noida, India, raided and shut down a fake call centre targeting United States citizens. During the raid 84 people were arrested and 150 computers, 13 mobile phones, 1 server, 42 printers and 1 luxury car were seized, along with the equivalent of around $25,000 USD in cash.

In the four month's the call centre was in operation it allegedly managed to steal funds from 600 US citizens, generating around $48,000 USD per day. The call centre used a leaked database of social security numbers (SSN's) to target their victims, initially by sending voice messages to inform them of their supposedly compromised SSN. The victims were then instructed to call back on a specified number, whereby they were made to believe their SSN had been used in criminal activity. They were then instructed to convert their bank account assets to cryptocurrency or gift cards, which would be held in escrow pending an investigation, in order to avoid account seizures. The call centre "employees" were all well trained and spoke with authentic sounding American accents thus convincing the victims they were genuine.

Africa Cyber Surge II

In a four-month joint initiative, carried out across 25 African countries, Interpol & Afripol worked together to identify almost 21,000 suspicious networks and arrest 14 suspected cyber criminals. The networks identified have been linked to losses in excess of $40 million.

As far as the specifics go, the authorities shut down 185 malicious IP addresses in Gambia, took down two darknet sites in Cameroon, 615 Kenyan malware hosting sites were taken down and two money mules in Mauritius were arrested along with a series of other arrests.

From a technical perspective the following resources were identified: 3,786 malicious command and control servers, 14,134 victim IPs linked to data stealer cases, 1,415 phishing links and domains, 939 scam IPs and more than 400 other malicious URLs, IPs and botnets.