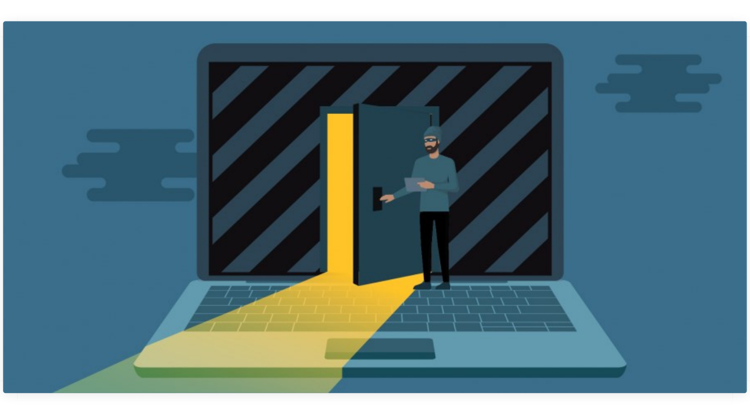
SilverTerrier – 2018 Nigerian Business Email Compromise

67,293 people reacted | 32 | 11 min. read
SHARE

By Unit 42
May 9, 2019 at 6:00 AM

Category: Unit 42
Tags: BEC, Business Email Compromise, Nigeria, Nigerian Prince, SilverTerrier



This post is also available in: 日本語 (Japanese)

Executive Summary

Over the past five years, Business Email Compromise (BEC) schemes have emerged as one of the most profitable and widespread activities amongst cyber criminals. This rapid rise has sparked alarm, recognition, and a call to action across both domestic and international law enforcement communities. In 2016 the Internet Crime Complaint Center (IC3) published its annual report highlighting BEC as a "Hot Topic" with single year losses estimated at US$360 million. A year later, BEC retained special recognition as a hot topic in the 2017 report which estimated US$670 million in annual losses. With rising public awareness and improved reporting mechanisms, law enforcement subsequently reported a 136% increase in losses between December 2016 and May 2018. Of greatest concern, the same announcement noted that global losses exceeded US$12.5 billion and impacted 150 countries in the five-year period from 2013-2018. Unfortunately, this trend shows no sign of slowing down with the recently released 2018 report noting that single year losses have now eclipsed US$1.29 billion.

Concurrently, Palo Alto Networks Unit 42 has actively monitored the evolution of this threat with a focus on Nigerian cybercrime. While BEC is a global threat, our focus on Nigerian actors provides insights into one of the largest subcultures participating in this malign activity given the country's historic ranking as a top five hotspot for cybercrime. In 2014, we released our first report 419 Evolution, documenting one of the first cases of Nigerians deploying malware for financial gain. Two years later, we released The Next Evolution of Nigerian Cybercrime, detailing a tremendous growth in malware adoption and assigning the code name "SilverTerrier" to these actors. In 2017, we observed the threat expand to hundreds of actors participating in BEC schemes with details released in The Rise of Nigerian Business Email Compromise. Over the past year, the number of SilverTerrier actors surpassed 400. Combined, these actors are now attributed to over 51,000 malware samples and 1.1 million attacks over the past four years. Leveraging this wealth of data, this blog outlines the most recent SilverTerrier malware trends and provides an overview of positive actions taking place across law enforcement and industry to combat this activity.

Attacks

Collectively, Nigerian cyber actors continued to prove their ability to deliver sizable year-over-year growth in attacks. In 2017, we observed an average of 18,294 attacks per month, representing a 23% increase from 2016. This period also included a new single month's record of 41,000 attacks in August 2017. In 2018, average attacks grew to 28,227 per month with surges in March and April both surpassing previous records (see Figure 1). This growth represents an alarming 54% annual increase and signifies that both the quantity and pace of attacks is increasing. Moreover, one should note that these numbers only reflect attacks against our customer base. Thus, while we assess that our metrics are representative of the global trends associated with this activity, it is very likely that the actual number of global attacks far exceeds our numbers.

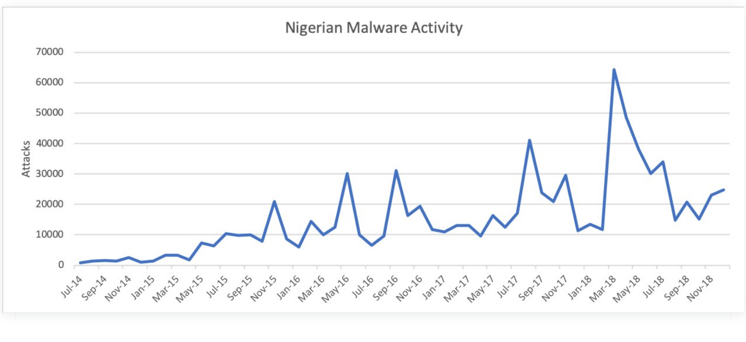


Figure 1. Nigerian malware activity from July 2014 through December 2018

In addition to impressive growth, Nigerian actors continue to launch their attacks against the breadth of all industry segments. Our data shows that the high-tech industry received the greatest number of attacks, climbing from 46k to 120k over the past year. The wholesale industry advanced to secure its place as the second most targeted industry, witnessing a 400% growth in attacks from 2017. Manufacturing also observed a sizeable increase in attacks from 32k to 57k but dropped one position to become the third most targeted industry in 2018. Finally, education and professional/legal services both witnessed sizable growth in attacks as the fourth and fifth most targeted industries, respectively.

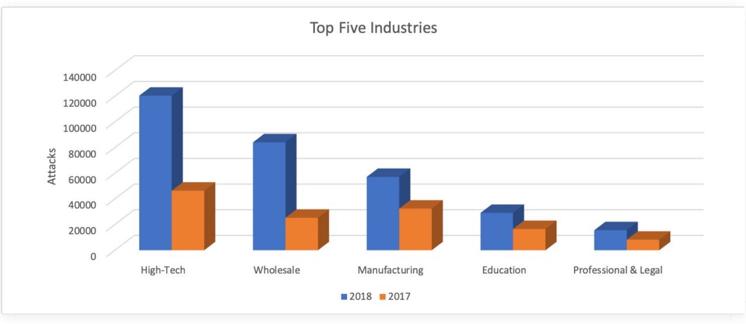


Figure 2. Top five targeted industries

Analyzing the delivery vectors used in these attacks produced a consistent ranking of the top five applications between 2017 and 2018. Email applications topped the list with SMTP, POP3, and IMAP securing the first, second, and fourth most common delivery applications, respectively. In terms of metrics, we observed malware in 219k SMTP sessions, 46k POP3 sessions, and 8.4k IMAP sessions. Web browsing remained the third most common delivery application with malware detected in 20k sessions while FTP ranked fifth with only 654 sessions. Comparatively, these metrics provide valuable insights for network administrators, informing the need for email-based detection capabilities in order to adequately defend against this threat.

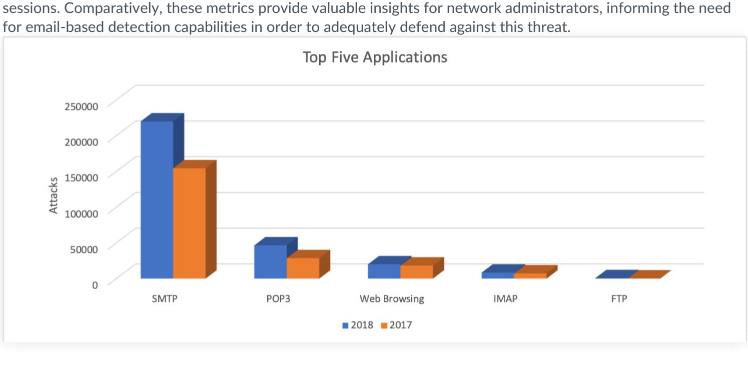


Figure 3. Top five delivery applications

Malware

SilverTerrier actors are gaining experience quickly as they adopt new technologies, techniques, and malware to advance their schemes. Over the course of the past four years, we tracked their adoption and use of 20 different commodity malware tools. Procured for nominal costs, these tools require minimal setup, and come preloaded with a variety of capabilities that enable actors to achieve their desired outcomes. Given that the antivirus community is often quick to identify and signature these tools, Nigerian actors frequently leverage a variety of constantly evolving "crypters" as a means to obfuscate the tools and circumvent signature-based detection capabilities. Comparing 14,694 SilverTerrier samples collected in 2018 against VirusTotal demonstrated an average detection rate of 53% across vendor solutions at the time of discovery. By the end of the year, subsequent measurements taken in early 2019 revealed that detection rates improved over time, but only by five percentage points, achieving 58% across all vendors. This low number lends credence to, and highlights the significance of, the threat that this malware employment technique poses to organizations relying on traditional signature-based detection capabilities.

Focusing on the individual tools, we continue to find that the adoption and employment rates of malware families rise and fall consistent with popularity, effectiveness, detection rates, availability, and other traditional market factors. Analysis of these trends can provide valuable insights for network administrators in terms of validating and tailoring network defenses for the most common threats. Of equal importance, these trends guide the cybersecurity industry in prioritizing detection capabilities while also enabling law enforcement to focus attribution and legal process against tool developers. In performing this analysis, we grouped the tools into two broad categories: Information Stealers and Remote Administration Tools, or RATs.

Information Stealers

AgentTesla, Atmos, AzoRult, ISpySoftware, ISR Stealer, KeyBase, LokiBot, Pony, PredatorPain, and Zeus are all commodity malware tools designed with a core information stealing component. Upon infection, they capture screenshots, passwords, or other sensitive files which are then transmitted to locations where they can later be retrieved by cyber actors. In most cases, these tools rely on simple command and control mechanisms such as uploads to web servers, FTP servers, and SMTP email connections. These common services blend in with normal network traffic and ultimately impede detection capabilities by traditional port/protocol filtering edge devices. However, this strength is also a weakness in that the malware control infrastructure is generally hard coded as a domain or email address. Once identified, this infrastructure can be taken down by service providers thus terminating collection and limiting the period of effective use for these tools.

Across the ten tools, Nigerian actors produced an average of 1000 unique samples of malware per month in 2018 (see Figure 4). Although substantial, this average represents a noteworthy 26% decline from the previous year. Our data suggests that the rapid growth experienced between 2014 and 2017 has reached its peak, plateaued, and is now in decline. While difficult to pinpoint the exact reason behind this phenomenon, it is likely that declining availability of tools, increased law enforcement efforts, advancements in the cybersecurity landscape, and increased adoption of RATs by SilverTerrier actors were all contributing factors.

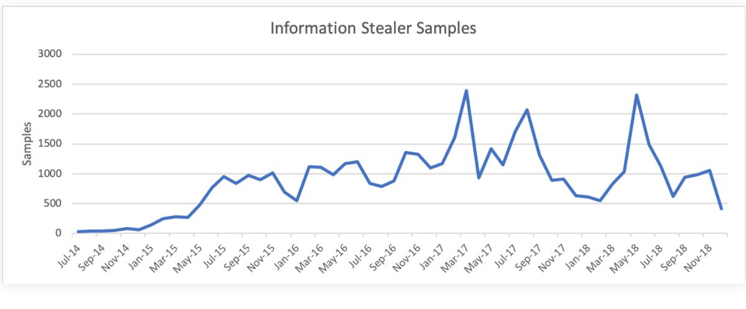


Figure 4. Information Stealer samples 2014-2018

Exploring the most popular tools in this category, we found that SilverTerrier samples were disproportionately associated with four of the ten tools seen in 2018. At the top of the list, we observed an average of 446 samples of Lokibot. Pony, which averaged 330 samples per month, maintained its popularity throughout 2018 likely due to its dual nature as a capability for stealing credentials and more importantly, its ability to download and install additional malware tools on compromised systems. Next, actors produced an average of 95 samples per month of AgentTesla, a small .NET keylogger. Finally, PredatorPain, a tool which has received multiple updates over the years, fell in popularity from its peak usage in 2016, but maintained a steady following of actors producing an average of 65 samples per month throughout 2018.

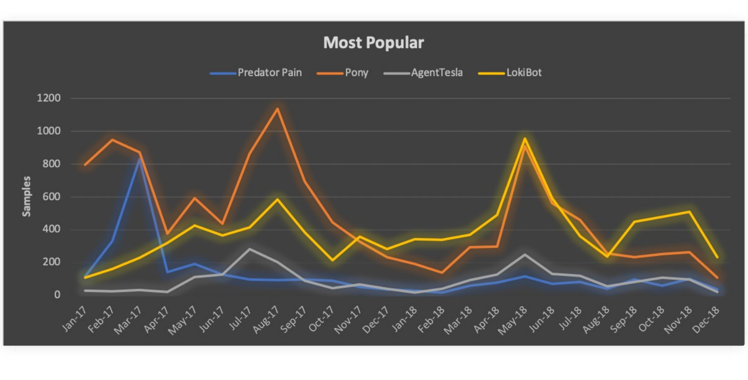


Figure 5. Most popular Information Stealers 2018

On the other end of the spectrum, our data shows that historically Atmos, AzoRult, KeyBase, ISpySoftware, and ISR Stealer were very capable tools, yet all have experienced dramatic declines from their peak usage rates. In comparison with the most popular tools, we observed an average of only 24 samples per month of ISR Stealer attributed to a hand full of actors in 2018 while the remaining capabilities ranged from two to 16 samples per month.

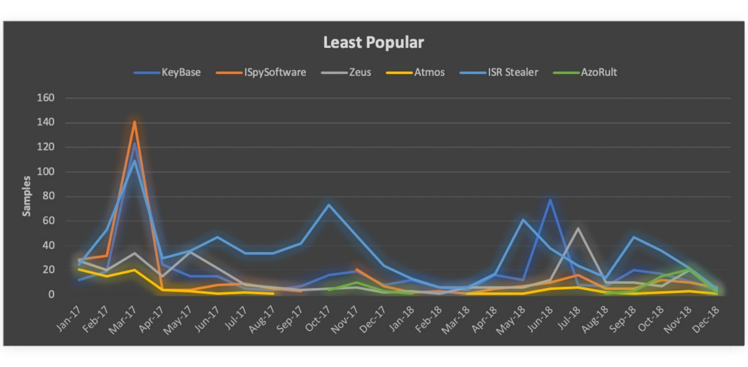


Figure 6. Least popular Information Stealers 2018

Remote Administration Tools

NetWire, DarkComet, NanoCore, LuminosityLink, Remcos, ImminentMonitor, NJRat, Quasar, Adwind, HWorm are all commodity malware tools that provide attackers with remote access to compromised systems. In doing so, these tools expand upon the basic data theft capabilities of information stealers and allow SilverTerrier actors to modify systems, access network resources, and perform functions on behalf of compromised users. This functionality is commonly leveraged to send malicious or fraudulent emails and access databases within victim organizations in hopes of monetizing their efforts. However, with greater capabilities comes greater complexity and these tools often require additional experience to deploy and operate. For example, the interactive nature of these tools demands steady connections to control servers that are often running on high number ephemeral ports. In order to protect the control servers, actors frequently rely on dynamic DNS and virtual servers rather than static domain registrations. This technique affords actors a layer of obfuscation making attribution more difficult while also extending the useable life of a malware sample, as dynamic DNS allows for transfer of control to new servers over time.

Evaluating Nigerian use of these ten tools in 2018, we observed an average production of 533 samples per month, representing a gain of 36% over the previous year. This sample rate is nearly half that of information stealers, yet the growth rate stands in stark contrast. Combined, the data suggests that Nigerian actors are moving away from legacy information stealers in favor of remote administration tools which provide greater capabilities to achieve their goals. Given these metrics, we assess that RAT adoption and deployment will continue to climb at a consistent rate throughout 2019.

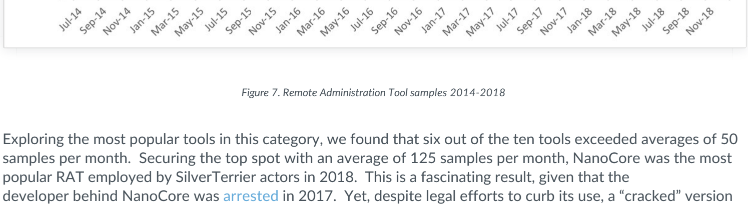


Figure 7. Remote Administration Tool samples 2014-2018

Exploring the most popular tools in this category, we found that six out of the ten tools exceeded averages of 50 samples per month. Securing the top spot with an average of 125 samples per month, NanoCore was the most popular RAT employed by SilverTerrier actors in 2018. This is a fascinating result, given that the developer behind NanoCore was arrested in 2017. Yet, despite legal efforts to curb its use, a "cracked" version of the tool remains available for free download on various forums across the internet, thus allowing for continued use. DarkComet and Netwire, both adopted back in 2014, followed in popularity with averages of 86 and 85 samples per month respectively. HWorm, originally released in 2013, has received developer upgrades over the years. Despite its history, our first confirmed use by Nigerian actors was in March 2018 and since then, we have observed an average of 70 samples per month. Finally, SilverTerrier actors continued to steadily employ Remcos, first seen in 2016, and Adwind, first seen in 2015, at average rates of 58 and 53 samples per month throughout 2018.

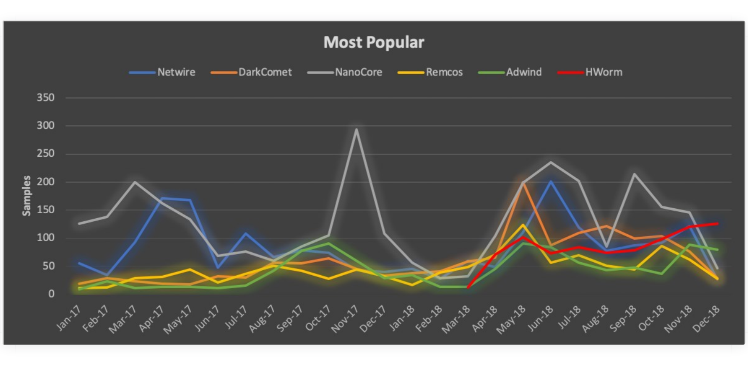


Figure 8. Most popular Remote Administration Tools 2018

Standing in contrast to the steady employment and rapid adoption of the most popular tools, we saw that ImminentMonitor, LuminosityLink, NJRat, and Quasar have lost popularity over the past year. Of the four, ImminentMonitor maintains a small but loyal following of Nigerian actors that produced an average of 24 samples per month. LuminosityLink, serves as a success story for law enforcement in that usage dropped from over 100 samples per month in early 2017 to an average of 18 samples per month in 2018 after the developer was arrested. Public attribution, attack metrics, and historical sales context provided in our February blog post aided law enforcement efforts in securing a guilty plea in July, followed by sentencing in October. Finally, Quasar and NJRat exist as anomalies, having never gained tremendous adoption rates amongst SilverTerrier actors, thus resulting in low averages of 8 and 6 samples per month, respectively.

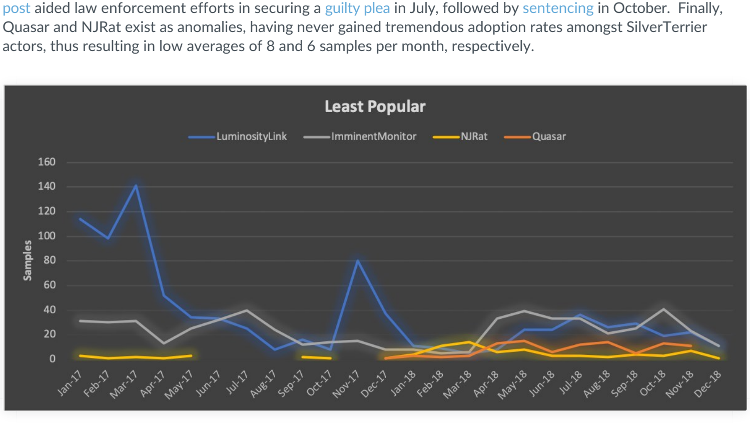


Figure 9. Least popular Remote Administration Tools 2018

A Year of Action

Despite the continued growth in attacks and US$12.5 billion in global loses attributed to BEC schemes over the past five years, there were also a series of positive actions that took place cementing 2018 as an important milestone in the battle against this threat. Arguably, the most noteworthy of these activities was the mobilization and unprecedented level of collaboration between law enforcement and private industry partners from the cybersecurity, technology, and financial sectors. While the foundation for this collaboration dates back to the first BEC conference hosted in 2016, this industry-led initiative has since transformed into an annual event that continues to pay dividends for all organizations involved.

One such dividend was realized in January 2018 when the Federal Bureau of Investigation (FBI) launched its first large-scale, coordinated effort to dismantle BEC operations globally. Over the course of six months, law enforcement officers participating Operation Wirewire arrested 74 individuals. Amongst them were 29 Nigerians arrested as a result of the FBI's close collaboration with the Nigerian Electronic Federal Crimes Commission (EFCC). Capitalizing on the success of the operation, the third annual BEC conference convened in July 2018. There, law enforcement organizations provided valuable feedback to industry partners and highlighted an expanding list of new relationships with international counterparts energized to tackle this threat.

Beyond law enforcement actions and in October 2018, Mr. Ronnie Tokazowski, the founder and administrator of the BEC collaboration group, graciously accepted the JD Falk Award on behalf of the group's 530+ members. This award specifically recognized the group's achievements on preventing millions of dollars in fraud through real-time, cross-industry collaboration, as well as efforts that resulted in the disruption of thousands of Nigerian scheme email accounts.

Combined, these two exemplars mark the beginning of a positive turning point as organizations look beyond individual defense activities towards proactive actions to combat the BEC threat. Where cyber actors previously acted with impunity, law enforcement has now demonstrated the resolve to coordinate with foreign partners in pursuit of these crimes. Nowhere is the success of this collaboration more evident than in Nigeria where the EFCC proudly posts on their public Facebook page photos of actors along with their associated charges.

Conclusions

Business Email Compromise (BEC) schemes are one of the most profitable and widespread activities amongst cyber criminals with recent reports quantifying global losses in excess of US$12.5 billion. Unit 42 monitors this threat through the lens of Nigerian cybercrime. In doing so, we active track more than 400 SilverTerrier actors attributed to roughly 51,000 malware samples and 1.1 million attacks over the past four years.

SilverTerrier actors remain a formidable threat to businesses worldwide, demonstrating a 54 percent increase in attacks in 2018. These actors predominately rely on email to distribute their malware with the most targeted industries being: High Tech, Wholesale, Manufacturing, Education and Professional/Legal Services.

Our data from 2018 shows that information stealing malware families remain in common use, with SilverTerrier actors producing an average of 1000 samples per month. However, the production of new samples declined 26% signaling a shift to more capable Remote Administration Tools which saw a 36% increase and an average production of 533 samples per month.

While BEC campaigns remain an active threat, Palo Alto Networks customers are protected in the following ways:

- WildFire® cloud-based threat analysis service and Traps™ advanced endpoint protection accurately identify samples associated with these malware families.
- DNS Security Service, Threat Prevention and URL Filtering identify all phishing and malware domains associated with these actors as malicious.

Users of AutoFocus™ contextual threat intelligence service can view malware associated with these attacks using the following tags:

Adwind

AgentTesla

Atmos

AzoRult

BilalStealer (ISR Stealer)

DarkComet

HWorm

ImminentMonitor

ISpySoftware

KeyBase

LokiBot

LuminosityLink

NanoCore

NetWire

NJRat

Pony

PredatorPain

Quasar

Remcos

Zeus

SilverTerrier

You can find a complete list of the malware domains associated with SilverTerrier actors on GitHub®.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.