SILVERTERRIER:

The Next Evolution in Nigerian Cybercrime

REPORT BY PETER RENALS & SIMON CONANT

PALO ALTO NETWORKS | 4401 Great America Parkway | Santa Clara, CA 95054
www.paloaltonetworks.com

Executive Summary

In July 2014, Palo Alto Networks® Unit 42 released its first threat intelligence report on Nigerian cyber actors. This report documented the observed evolution from traditional 419-style email scams to the use of commodity malware for financial gain. Over the past two years, Palo Alto Networks has continued to collect thousands of samples of malware associated with these actors. With this wealth of data, Unit 42 recently launched an unprecedented analytic effort to develop a current assessment of the size, scope and complexity of this threat.

Applying advanced analytics across more than 8,400 samples resulted in the identification of over 500 domains supporting malware activity and roughly 100 unique actors or groups, which we continue to track under the code name "SilverTerrier." This data exhibited that these actors' ability to distribute malware has grown steadily over the past two years to its current rate of 5,000–8,000 attacks per month. Moreover, using email as the primary means of distribution, the majority of these attacks were focused against the high technology, higher education and manufacturing industries.

While these attacks originate from actors with varying degrees of technical expertise, all of the actors continue to rely on commodity malware tools, which require minimal infrastructure to set up and can be acquired on underground forums at nominal costs. Historically, this fact has been used to draw assumptions regarding the technical competence of these actors; however, given our findings, we believe these assumptions may warrant reassessment.

Through our analysis, it has become clear that Nigerian cyber actors have demonstrated significant growth in size, scope and capability over the past two years. They have learned how to successfully apply simple malware tools with precision in order to create substantial losses ranging from tens of thousands up to millions of dollars for victim organizations, and they have broadened their scope well beyond targeting unsuspecting individuals. As a result, these actors now pose a formidable threat to businesses worldwide.

History

Over the past three decades, the world has witnessed an evolution of fraud stemming from criminals operating within Nigeria. Starting in the early 1980s, millions of paper letters were distributed to unsuspecting recipients all over the world. These letters often followed the template of the historical, advance-fee type of scam in which recipients were enticed to transfer funds or send their financial information in exchange for generous returns or compensation. The stories behind these paper letter scams continued to evolve through the 1980s, and with Laws of the Federation of Nigeria being passed under military decree in 1990, they soon became known as "419 scams" based on the section of criminal code that covered fraud.

In the mid-1990s, telecom providers within the country began offering internet services, and it didn't take long for 419 scams to make the leap to this new medium. The availability of email allowed scammers to rapidly tailor their schemes based on current events, interact in near real-time with potential victims, and ultimately led to a significant increase in the magnitude of their distribution.

This trend continued to climb and, in 2008, the Federal Bureau of Investigation released its annual Internet Crime Report listing Nigeria as third in the world for conducting cybercriminal activity. While the country's position on the list has fluctuated over the years, it once again claimed the number three position in last year's Internet Crime Report.

Over that same period, tactics and techniques continued to evolve, shifting gradually from the traditional 419 emails to schemes involving full websites designed to impersonate legitimate entities. In July 2014, Unit 42 released a report called 419 Evolution documenting that Nigerian cybercriminals had officially incorporated malware into their schemes.

Tools & Trends

Since 2014, Nigerian actors have been linked to various popular malware tools, including Zeus, DarkComet and others. All of these tools have something in common: they are commodity malware tools that require minimal infrastructure to set up and can be purchased at nominal costs on underground forums. Traditionally, this fact has been used to justify assessments that suggest these actors lack the technical aptitude required for more advanced tools. But our research suggests that these tools may be chosen intentionally to support easy scalability among a distributed actor network similar to an organized crime model.

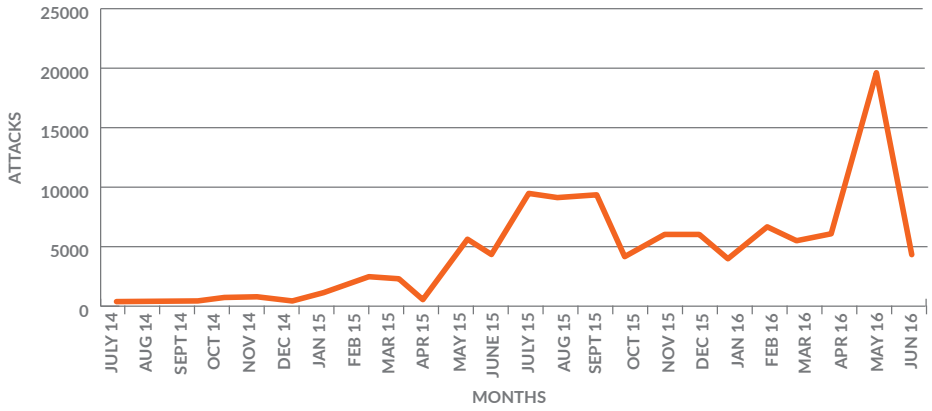
As these tools rise and fall in popularity (and more importantly, as detection rates by antivirus vendors improve), SilverTerrier actors have consistently adopted new malware families and shifted to the latest packing tools available. Given this trend, the focus of this report is on the Predator Pain, ISR Stealer, Keybase, ISpySoftware and Pony malware families, due to their current popularity among Nigerian actors.

These five tools range in cost from free to $35, depending on the version, capabilities and licensing requirements desired by the actor. Each tool produces malicious executable files that are designed either to provide remote access to a system or to steal credentials from a victim, with the majority of these variants targeting Microsoft® Windows® operating systems.

While the malware itself is not overly complex, these actors routinely rely on packing software or "crypters" in order to obfuscate the code so that it won't be identified by traditional antivirus solutions. In doing so, they are able to maintain a core set of cheap malware tools and infrastructure while only paying for secondary tools designed to disguise their malware as benign files. To that end, some actors have been observed employing the latest crypters they can gain access to, often using a tool for only a few weeks before upgrading or shifting to the next available tool.

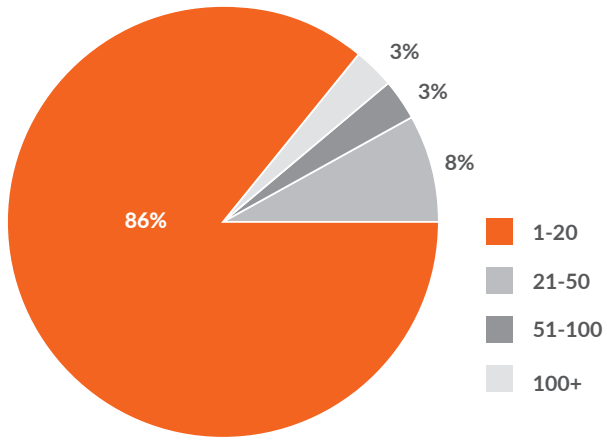
Analyzing their use of the five core malware tools, the ability of SilverTerrier actors to distribute malware has grown steadily over time to its current level of 5,000–8,000 attacks per month. However, in May 2016, they demonstrated the added ability to surge distribution efforts by launching nearly 19,000 attacks in one month.

Nigerian Malware Activity



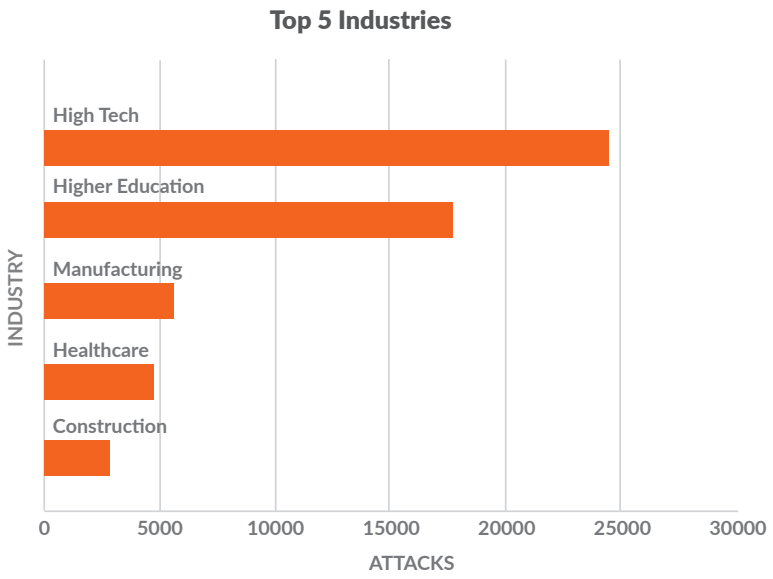
While the malware itself can be distributed at scale and in far greater numbers than observed above, the benefits of doing so are often diminished for these actors. As a basic principle, there is generally a correlation between the amount of malware distributed and the time it takes for antivirus vendors to identify and block it. Thus, these Nigerian actors have refined their attack methods over time from sending malware in bulk across the internet to a more focused, deliberate and targeted approach. Specifically, our data showed that 86 percent of the malware samples analyzed were observed in 20 or fewer attacks against Palo Alto Networks customers.

Number of Times Samples Were Observed



These targets fall across all lines of industry; however, the data shows that Nigerian actors are predominately targeting organizations in high technology, higher education and manufacturing. This pattern represents a significant departure from traditional

Nigerian criminal activity, which historically has been focused on individuals and petty crime, to a much more substantial threat for the international community, targeting everything from small businesses to major corporations.



Who Are They?

Using AutoFocus™ contextual threat intelligence, combined with advanced analytic practices, Unit 42 is currently tracking roughly 100 Nigerian cyber actors responsible for operating the infrastructure associated with the five malware families identified above. These actors were predominately identified using domain registration details, which, in many cases, enabled Unit 42 to link these actors directly to their social media profiles. Performing this practice on a large scale has produced tremendous insights into the size, scope, motivations and interactions of these actors.

What Do We Know About These Actors?

They are comfortable. The actors we have identified are individuals predominately from the cities of Owerri, Lagos, Enugu, Warri and Port Harcourt in the southwest/coastal region of Nigeria. The majority of these actors continue to reside in these cities, close to friends and family, where they live comfortably on the proceeds of their criminal activity (particularly given the favorable exchange rate between foreign currency and the Nigerian naira). Additionally, some of the more successful actors have begun traveling abroad to European and Asian countries. The two most popular locations appear to be the United Kingdom and Malaysia where many of these individuals quickly reestablish their criminal operations.

They are educated. Many of them have attended technical secondary schools and have gone on to obtain undergraduate degrees from the Federal University of Technology (FUTO) or other regionally aligned university systems offering technical degree programs.

They aren't kids. These individuals range in age from late teenage years to adults in their mid-40s, thus representing a wide range of generations participating in this criminal activity. Historical domain data revealed that the older generations consist of

individuals who were once successful at launching 419 email campaigns and impersonating legitimate government, financial, manufacturing and international freight organizations to support their schemes. The younger generations represent those graduating fresh out of the universities, who are beginning their criminal careers with malware, while building off the scamming techniques developed by the older generation. Together, these groups are blending their tools and techniques to achieve their goals. However, while the tools these actors use are relatively simple, their employment of the tools indicates a clear level of refinement, precision and sophistication.

They aren't necessarily hiding. While a small subset of the actors go to great lengths to conceal their identities, the culture within Nigeria tends to provide a permissive environment for these types of illicit activities. Scams, fraud and corruption are viewed as a way of life, and as a result, the majority of these actors apply little effort toward maintaining anonymity. Instead they frequently combine fake names, aliases or nicknames with local addresses, phone numbers and personal email accounts in order to register their malicious domains. In most cases, these attributes can easily be linked back to their well-developed online social profiles. These profiles include Google®, Hotmail and Yahoo!® email addresses, as well as social media accounts on Facebook®, Google+™, YouTube™ and, to a lesser extent, LinkedIn® and Twitter®. Across their social media accounts, many of these actors claim to be "self-employed," while their profiles document their education, their associates, and openly flaunt their success through pictures of nice cars, gold chains and foreign currency.

They are becoming organized. Various actors are communicating, cooperating, and sharing tools and techniques. The individuals who maintain the technical aptitude to establish malware infrastructure either operate individually or lead teams of less-skilled actors. Those operating individually are connected through social media to other local actors with similar skills, as well as international actors using the same tools. Likewise, those leading teams maintain the same social network connections but are often referred to as "boss" on their social media profiles by the actors they support. A prime example can be seen in a recent threat report released by SecureWorks® in which one actor was discovered to be supporting upward of 30 subordinates. In this arrangement, the boss typically registers the malware infrastructure, establishes a folder structure to support each subordinate, and then provides training on the tools, likely in exchange for a portion of the profits.

While Unit 42 has identified roughly 100 individuals with the skills required to establish this type of malware infrastructure, our data similarly showed that a small subset of these actors appear to be leading teams of between 4 and 30 subordinate actors.

Social Media Networks

The majority of SilverTerrier actors are very active on social media, with the two most prevalent networks being Facebook and Google+. However, while both of these networks provide a means for individuals to express themselves and share ideas, Nigerian actors use them to accomplish two distinctly different purposes.

For these actors, Facebook accounts typically represent legitimate depictions of their personal lives. These profiles contain their true names, links to family members, and connections to friends from their high school, college and hometown. In that mix, one typically finds links to local law enforcement, educational mentors and community religious leaders, as well as their criminal peers and subordinates. Additionally, while these profiles often contain images flaunting wealth and success, they tend to contain very few blatant links to criminal activity or tools. Of course, there are a few instances in which connections claim affiliation with the Anonymous hacking group, or users are attempting to sell malware tools on their wall, but by and large, this activity is generally an exception rather than the norm on Facebook's platform.

Figure 1 + Examples of SilverTerrier actors flaunting success on Facebook

Conversely, the actors' Google+ profiles appear to be built for the purpose of supporting their illegitimate activities. While their Facebook profiles are linked to their personal email addresses, their Google+ profiles are most often linked to email accounts used to register malicious domains. As a result, these accounts typically contain fewer than ten connections, most of which are to other nefarious individuals or organizations. Furthermore, this platform serves as a conduit in connecting local criminals to international tools and capabilities while maintaining some degree of privacy and anonymity. By mapping this network, Unit 42 has successfully identified the linkage between Nigerian actors and such tools as NanoCore Remote Access Trojan, HawkEye Keylogger, Aegis Crypter and Orway Crypter.

More importantly, this mapping effort has enabled the identification of a small number of individuals who appear to serve as the connective tissue between various subsets of Nigerian actors and the tools they use. While these individuals have not been linked directly to malware infrastructure themselves, conclusions about their

importance and overall role with respect to Nigerian cybercrime can be deduced simply from their connections. This analysis thus informs a generic understanding of the network that looks like this:

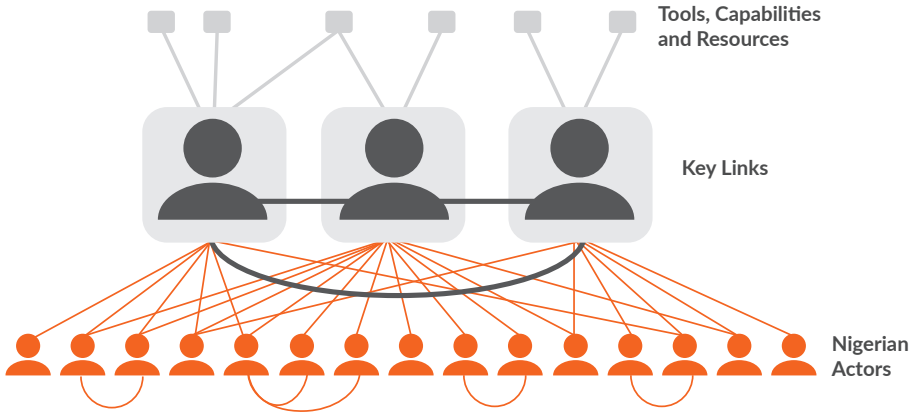


Figure 2 + **Simplified depiction of Google+ social network**

With an understanding of this generic model, it becomes possible to create products that blend the information provided by both platforms. Doing so produces a wealth of insights into these criminal organizations. Most notably, this method can be used to establish connections between aliases on Google+ and actors' true identities on Facebook. Once these links are established, second order analysis can easily be conducted to identify commonalities, degrees of separation, and levels of influence between organizations and individual actors. One such example can be seen below:

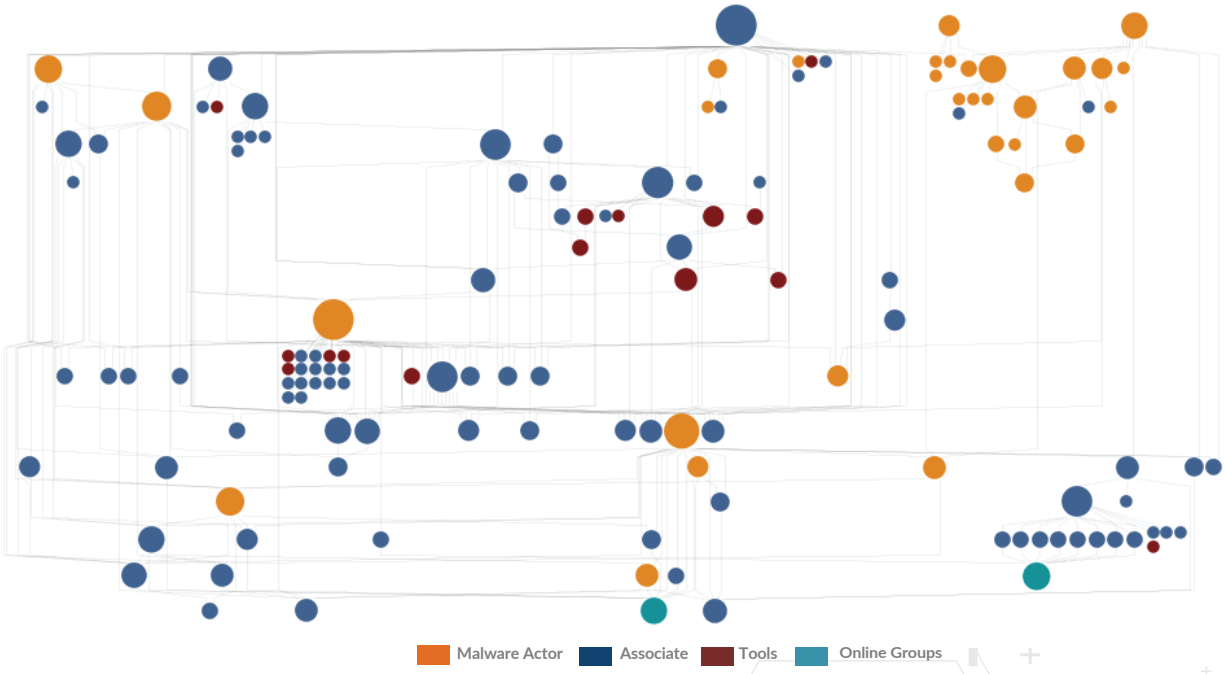


Figure 3 + **Blended Link Analysis**

Current Tactics

At any point in time, many of these actors are engaged in multiple categories of scams ranging from their traditional 419 emails, to fake websites, to the most recent malware initiatives. Thus, in order to account for the range of their activities, it becomes necessary to discuss the domains that SilverTerrier actors are building to support their activities. These domains can be grouped into three generic categories: self-named, fake organizations, and impersonation of legitimate organizations.

Self-Named

These domains either have a personal meaning to the actor that is not readily apparent to an outside observer, or they contain names that are linked directly to the actor's identity. For example, an actor using the alias of "Spy" and an organization of "Kabospy" established the following three domains: Kabospy[.]com, Kabospy1[.]com and Kabospyz[.]com. In this case, these three domains were all used to support malware activities; however, this category has also been observed as having the widest scope of use overall. Depending on the specific actor in question, these domains range in use from seemingly legitimate activities, to frauds and scams, to supporting malware.

Fake Organizations

The concept of standing up fake organizations is a trend that expanded in the gap between traditional 419 email scams and their adaptation to malware, but it remains popular among Nigerian actors today given the versatility that these sites provide. These domains are typically configured with a full-service website in order to present a legitimate front to their viewers. Historically, this concept was focused on the creation of fake financial institutions in order to defraud unsuspecting victims. Recently, we have seen instances of this trend expanding to incorporate other industries, including manufacturing companies and, in some instances, charities in order to support both fraud and malware campaigns. It is also important to note that, over the course of the past few years, these websites have evolved in complexity. Early attempts by the actors to develop these websites often included grammatical errors and clunky interfaces that led average computer users to question the nature of the websites. Modern versions now demonstrate an enhanced level of web design proficiency and project a more professional appearance.

As an example, the following two websites are registered to the same Nigerian actor. Looking at each website independently, both appear to be professional products. Links are active, the search bar works, and they contain contact information, a map of London, pictures, and biographies of company leadership. However, upon inspecting the websites as a pair, it quickly becomes evident that they are mirror images of one another, with only slight discrepancies. References to "Mg & Associates" stand out, and the profiles of company leadership also prove to be suspect as they are reused across various websites owned by this actor.

Figure 4 + www.kaequipments[.]com

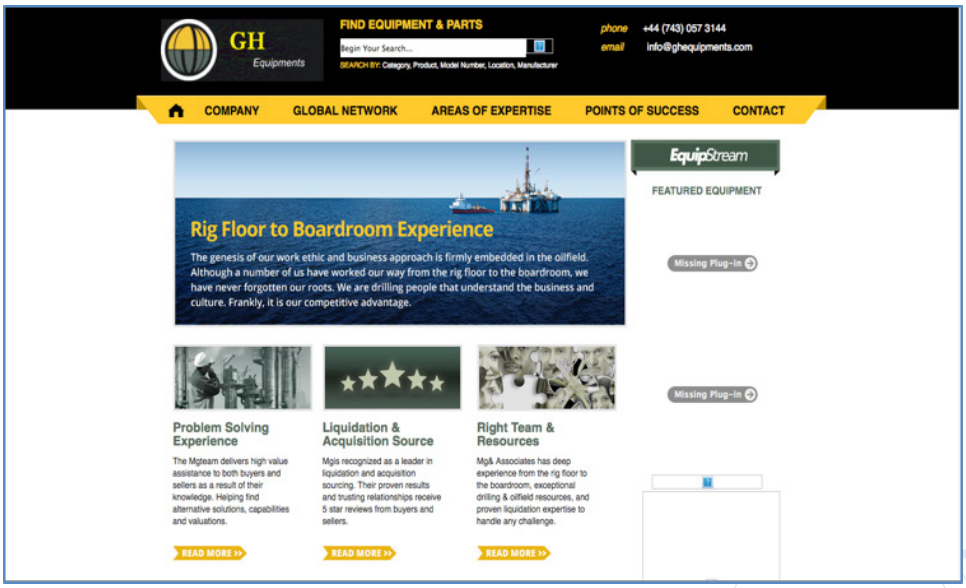


Figure 5 + www.ghequipments[.]com

Separately, this next example represents an illegitimate charity. While the site presents an appearance consistent with what one might expect from a charitable organization, a closer look reveals a number of discrepancies that should raise alarms. For contact information, the main office in the United Kingdom is actually a facility that provides temporary and virtual office space. Similarly, their location in the United States is a non-existent address that resolves to a parking lot associated with a major corporation. Lastly, the donation page indicates that it is under construction, but visitors are encouraged to make donations through Western Union or MoneyGram.

Figure 6 + www.vintageorphanagelimited[.]com

Impersonating Legitimate Organizations

The last category is comprised of domains that are designed to impersonate legitimate organizations. Organization names for these domains are slightly modified from their real-world counterparts, and in most instances, the domains do not contain functioning user-friendly websites. Instead, these domains are used to host email services in support of malware distribution, or they provide command-and-control (C2) services for malware to post stolen user credentials.

SilverTerrier actors have been observed using this technique to impersonate organizations in the healthcare, education, sports, technology, public transportation, international freight and finance industries. More concerning is the fact that recently this technique has expanded to include the full spectrum of government organizations, including law enforcement, military and diplomatic entities.

The following represents a small sample of these domains registered by Nigerian actors to support fraudulent activities:

Impersonated Organization	Fraudulent Domain
Samsung	Samrsung[.]com
Adobe	AdobePDFUpdate[.]com
Western Union	WesternUnion-Home.co[.]uk
Interpol	InvestigateInterpol[.]net
Federal Bureau of Investigation	FBIGov[.]Org
United States Army	ArmyDepartment[.]us

Email Distribution

Of the thousands of samples analyzed by Unit 42, the overwhelming majority of malware was distributed to target organizations through email. These email messages followed two distinctly different patterns depending on the target of the attack.

When targeting individuals, these emails provided a direct value proposition to their targets. In this case, emails generally originated from impersonated shipping, banking or law enforcement organizations. For example, when shipping companies were used, emails informed their recipients that a package was pending delivery, and attached was a malware file disguised as a tracking confirmation document. Emails appearing to come from banking organizations often contained subjects indicating an issue pertaining to a refund or transfer of funds. When law enforcement organizations were used, the emails contained attachments that were crafted to look like evidence relating to the target. Over a period of five days in May 2016, this specific approach was seen in over 6,800 emails sent with a subject of "Warning from the FBI" and an attachment called "Your File.exe," which was, in fact, Predator Pain malware.

Separately, when targeting businesses and large organizations, the emails were sent from impersonated business partners or those seeking to initiate future business prospects with the target organization. Additionally, in cases of Business Email Compromise (BEC), emails originated from compromised accounts internal to the organization. While these emails contained a wide variation of subjects and filename combinations, they all tended to align with the general themes of invoices, purchase orders, new orders, and requests for quotes.

Motivation

Business Email Compromise (BEC) and Business Email Spoofing (BES) are two attack techniques that have recently gained popularity among SilverTerrier actors. In both approaches, the actors employ methods designed to fool victims into authorizing electronic bank transfers. The subtle difference between the two is that BES involves the use of fake email accounts, whereas BEC attacks typically use compromised accounts or systems from victim organizations. Common usage of the

History has shown that the behavior of these actors has traditionally been financially motivated for personal gain. Fraudulent websites and 419 email scams both provide a steady stream of income consistent with their motivations. However, the success of these tactics is generally constrained by the overall wealth of their individual victims. Conversely, the allure of BEC is that it targets organizations rather than individuals. As a direct result, the return on investment for targeting organizations is generally significantly higher.

That said, our dataset enables the identification of individual attacks and the techniques used, but it lacks the details associated with the actors' monetization efforts, as those are typically only known by the victim organizations. However, given the fact that these techniques are known to be prevalent among Nigerian actors, and their domain registration activity is also indicative of BEC activity, it is our assessment that these actors are likely using the methods described above in order to support BEC schemes for personal gain.

Victims

The ability to provide accurate metrics for the victims of these attacks presents a unique challenge for cybersecurity analysts. This information is clearly valuable, as it supports the capability to quantify the level of success being achieved by Nigerian actors. However, the issue lies in distinguishing between individuals and organizations that were targets of these attacks, as compared with the organizational systems that were actually compromised by the malware. Most security vendors have ample data on which of their customers were targeted and how those attacks were launched. Yet, the ability of a security vendor to track victim metrics depends entirely on the victim's 1) ability to identify the malware infection, and more importantly, 2) willingness to acknowledge and report the compromise in an environment where doing so often results in negative impacts to their business model. Given these constraints, drawing conclusions concerning victims and the overall success rates of Nigerian actors is best achieved through a review of recent reports, law enforcement actions, and any information that can be obtained from malicious domains.

As a starting point, the FBI's Internet Crime Complaint Center (IC3) publishes an annual report that documents the trends associated with United States' victims who have reported losses as a result of criminal cyber activity. While these reports do not draw distinctions between the perpetrators of malware losses, they do outline specific metrics associated with traditional 419 scams, which shed light on the historical successes that these actors have seen. In 2001, Nigerian 419 scams represented 15.5 percent of the total reports received, with the average loss per victim being $5,575. Over the years, these numbers have declined as internet users have become more aware of the threat. In 2008, Nigerian actors represented only 7.5 percent of the total reports received with the average loss dropping to $1,650 per victim. While this seems like a positive trend, last year's report sought to provide additional quantification in order to draw contrast between average losses and total losses. Overall in 2015, there were 30,855 victims of 419/Overpayment scams,

losses. Overall in 2015, there were 30,855 victims of 419/Overpayment scams, resulting in losses in excess of $49 million. While those numbers are significant, the gains achieved through current malware and BEC schemes appear to be far greater. On August 1, 2016, Interpol released a press report detailing the arrest of a Nigerian actor named "Mike." According to the report, he is believed to be responsible for worldwide losses in excess of $60 million with over $15.4 million originating from just one victim.

Separately, on August 4, 2016, researchers from SecureWorks released a report identifying another group of Nigerian actors actively using malware to support BEC activity. In this case, one of the criminals was infected with the malware, thus affording the researchers a rare glimpse into the inner workings of the criminal organization. What they found was that the group had one individual who provided all of the technical support, infrastructure and training to more than 30 subordinates. Combined, this one group has gains estimated at $3-6 million per year, with an average loss for victim businesses of $30,000 to $60,000.

Shifting focus to the victims themselves, a review of the publicly available information hosted on active, but misconfigured, malware servers provided many interesting insights. While this approach only worked on a very small subset of the over 500 malware domains associated with these actors, the results showed that, on average, each domain contained victim data for between 5 and 15 organizations, thus informing a rough estimate of potentially 2,500 to 7,500 victims worldwide.

The majority of the victims were located in the Middle East and Asia, with a smaller subset in Europe and North America. All of the victims ran Microsoft Windows operating systems, many of which contained traditional endpoint antivirus solutions. Additionally, several of these systems were observed to contain timecard, billing and inventory software.

In almost every case, the victims were individual accounts on organizational and business computers rather than personal computers. In some cases, the malicious emails were sent to generic business accounts (info@organization[.]com), and in others, they were sent to specific users (user@organization[.]com). These emails originated from a wide array of sources to include spoofed and compromised accounts. For example, in one instance, the malicious email originated from an account appearing to belong to a foreign law enforcement official.

The victim organizations also ranged in size from small to medium-sized businesses with both local and global footprints. These organizations largely aligned with manufacturing, construction and other sales-oriented industries. However, while Nigerian actors focus their malware efforts against targets they believe to be profitable, this activity is sometimes indiscriminate and can result in significant secondary impacts to the international community. For example, one such victim identified by Unit 42 was an organization that serves as the intermediary between international telecom providers and their national government, in order to shape domestic policy. In cases such as these, the risks to society become an order of magnitude greater, ultimately placing these cyber actors on a different playing field from those traditionally thought of as low-level cybercriminals.

Conclusions

Over the past two years, Nigerian cybercriminal activity transitioned from 419-style scams to the active deployment of malware. What started as a small group of actors in 2014 has now grown to over 100 individuals, resulting in substantial year-after-year growth in this line of criminal activity.

Over the same period, multiple security vendors have produced reports documenting the actions of individual Nigerian actors and groups. Given the evidence available, these reports often implied a correlation between the simplicity of the malware tools used and the overall competence of the actors. Because of this trend, if CEOs were to ask their IT staff today whether they would consider Nigerian actors to be a threat, the answer they would likely hear is: "No, they use unsophisticated tools that are both easily detected and defeated." Yet, when the scope of research is expanded beyond a singular case to encompass more than 100 actors and groups, Unit 42 has found evidence that suggests the contrary. Simple tools being employed with a degree of precision and mastery should be worthy of concern, as they present a considerable threat.

While next-generation security solutions are highly effective at identifying Nigerian cybercriminal activity, traditional antivirus solutions are far less successful. An analysis of over 8,400 malware hashes submitted to VirusTotal showed an average identification rate of only 52 percent across vendors. This presents challenges to businesses worldwide that rely on legacy endpoint products alone to protect their employees when traveling outside the more sophisticated protections corporate networks typically provide.

Additionally, these actors are becoming organized; they are no longer individuals and small groups operating independently. Instead, SilverTerrier actors are using social media platforms to develop complex networks in support of their illicit activities. These networks provide a means to efficiently share tools, techniques and best practices. Furthermore, these efforts have enabled these actors to develop links to international criminal groups while also providing an opportunity for them to obtain the latest malware, packing software and tutorials. In this sense, they have begun to demonstrate traits indicative of small-scale organized crime.

Finally, these attacks have matured. Businesses have become the primary focus of Nigerian cybercrime, and the losses have already proven to be substantial. Proof of an individual actor's ability to steal $60 million, as well as evidence that groups using these techniques have been successful at stealing $3–6 million annually, should be considered a measure of their criminal competence.

Because of these traits, it is our assessment that Nigerian actors have demonstrated a clear growth in size, scope, complexity and capability over the past two years, and as a direct result, they should now be regarded as a formidable threat to businesses worldwide.

Protection & Mitigation

The best defense against these evolving threats is a security posture that favors prevention. Customers of Palo Alto Networks are protected from this threat in the following ways:

1. Domains used by these actors have been flagged as malicious in Threat Prevention.
2. WildFire™ threat analysis service accurately identifies samples associated with these malware families.

In addition to these protections, organizations are also encouraged to review the controls they have in place to prevent successful phishing attacks. Reeling in Those Pesky Phishing Attacks is a great resource that provides a list of best practices. However, more specifically, network security staff should also take steps to identify the individuals within their organizations who manage "info@companyname[.]com" and similar accounts as well as the individuals who manage sales functions with new clients. Given the tactics employed by Nigerian actors, special attention should be given towards ensuring controls are in place to protect those employees from tailored phishing attempts and malware disguised as new orders.

AutoFocus users can view malware associated with these attacks using the PredatorPain, ISR Stealer, KeyBase, ISpySoftware and Pony tags or the SilverTerrier campaign tag.

A complete list of the malware domains associated with SilverTerrier actors can be found on GitHub.

unit42

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com