SILVERTERRIER:
THE RISE OF NIGERIAN BUSINESS EMAIL COMPROMISE

PALO ALTO NETWORKS | 3000 Tannery Way | Santa Clara, CA 95054
www.paloaltonetworks.com

paloalto NETWORKS®

Executive Summary

In July 2014, Palo Alto Networks® Unit 42 released its first threat intelligence report, 419 Evolution, detailing the adoption of malware among a small group of Nigerian cyber actors. This shift represented a significant evolution from traditional 419-style email scams to the use of commodity malware for financial gain. Two years later, in 2016, Unit 42 launched an unprecedented analytic effort to characterize the adoption of malware across this threat group in our report "SilverTerrier: The Next Evolution in Nigerian Cybercrime." The results of that work identified substantial growth, with more than 100 actors or groups using five popular commodity malware tools to deliver thousands of attacks per month globally.

Since the release of that paper, Palo Alto Networks has continued to monitor the evolution of this threat group.

We have increased the scope of our analytic effort to include 15 commodity malware families employed by Nigerian actors. We also have now attributed more than 30,000 samples of malware to roughly 300 unique actors or groups that we continue track under the code name SilverTerrier. In the past year, these actors have conducted an average of 17,600 attacks per month, demonstrating a 45 percent increase from 2016. While simple commodity information stealers remain the most popular and widely deployed, there has been notable growth in the adoption of more complex remote administration tools, or RATs.

Despite continued increases in both attacks and malware production, we found the number of active threat actors during a given month has begun to stabilize, suggesting improvements in terms of efficiency. Additionally, we have observed that these actors continue to demonstrate increased organization. The social connections between these actors have become more robust and complex through leveraging social media platforms to promote their networking efforts.

Through our analysis, it remains clear that Nigerian cyber actors will continue to expand their attacks in terms of size, scope and capabilities. According to law enforcement organizations, the exposed losses to businesses worldwide from these threat actors are now estimated to be more than US$3 billion. Given the substantial risk these actors pose, we present techniques to enable large-scale attribution efforts to combat this threat. In doing so, we demonstrate a repeatable and sustainable process to identify SilverTerrier infrastructure and put preventive measures in place prior to the first samples of malware reaching our security products.

History

Over the past decade, Nigerian cybercriminals have become notorious for advanced-fee-style schemes, such as the well-known Nigerian Prince scam. Also known as "419 scams," based on the section of Nigerian criminal code that covers fraud, these schemes have historically leveraged email as a means to entice victims into transferring funds in exchange for the promise of generous returns. Although they were successful for several years, public awareness combined with anti-spam efforts have degraded the effectiveness of these campaigns.

To adapt to changes in the cyber landscape, some Nigerian cybercriminals pursued efforts to develop fake websites to impersonate organizations and dupe unsuspecting victims. Always looking for an edge, other actors turned to malware as a means to enhance access to potential victims. In 2014, Unit 42 released a report titled "419 Evolution" that documented one of the first known cases of Nigerian cybercriminals using malware for financial gain.

In 2016, Unit 42 launched an unprecedented analytic effort focused on developing a modern assessment of the size, scope and complexity of this threat. The resulting report identified substantial growth in the number of actors employing malware, the rate of malware delivery and the motivations behind these attacks. Most notably, in two short years, Nigerian actors evolved from using malware for simple financial gain to employing malware as part of complex Business Email Compromise, or BEC, schemes, which they refer to as "Wire Wire" scams.

These scams have proven to be tremendously profitable for cybercriminals. In the 2016 Internet Crime Report published by the FBI, BEC was specifically highlighted as a "Hot Topic", having been attributed to more than US$360 million in losses and gaining status as its own category of attack. A few months later, in February 2017, the FBI published a press release revising its estimates and stating that "Since January 2015, there has been a 1,300 percent increase in identified exposed losses, now totaling over $3 billion." Recognizing the significance of this threat group, Unit 42 continues to track the evolution of Nigerian cybercrime under the code name SilverTerrier.

Attacks

Starting with their ability to distribute malware, Nigerian cyber actors as a whole continue to demonstrate substantial year-over-year gains. In 2016, we observed an average of 12,200 attacks per month, with surges exceeding a rate of 30,000 attacks on two separate occasions. In comparison, over the past year, the average rate has climbed to 17,600 attacks per month, signaling a 45 percent increase. During the same time period, the attackers' ability to surge also increased, peaking at just over 41,000 attacks observed in August 2017 (see Figure 1). These metrics only provide insight into attacks against our customer base: to that end, we acknowledge the actual rates of attack worldwide likely exceed our metrics. Nevertheless, we believe the trend lines associated with our data set are representative of annual growth rates and emblematic of the pervasiveness of this threat group.

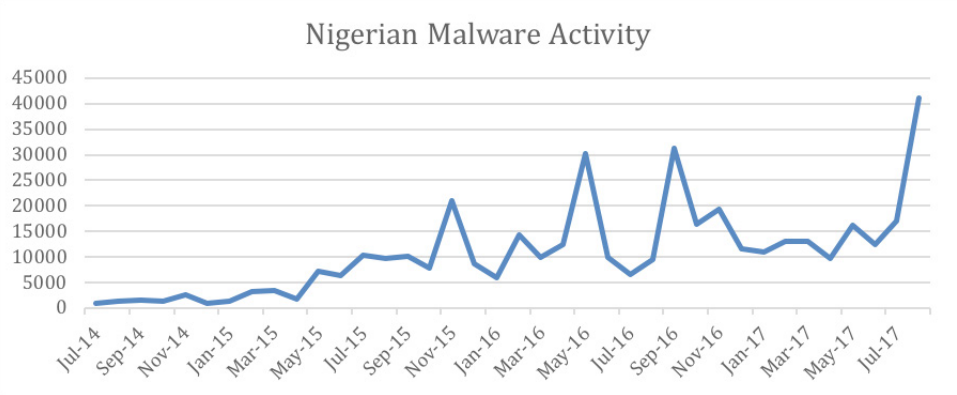

Figure 1 + Nigerian malware activity from July 2014 through July 2017

Tools and Trends

Individually, SilverTerrier actors continue to demonstrate varying degrees of technical proficiency, ranging from novice to highly experienced. However, as a group, these actors continue to exhibit noteworthy year-over-year technical growth as they adopt new tools and techniques. Over the past three years, they have employed a total of 15 different malware families to support their illicit activities. Although the use of each malware family may rise and fall consistent with its popularity, capabilities, availability and detection rates, all the families share a commonality in that they are commodity malware tools that can be procured for nominal costs. To explore their use in more detail, we grouped the tools into two broad categories: information stealers and remote administration tools, or RATs.

Information Stealers

Predator Pain, Pony, KeyBase, ISpySoftware, ISR Stealer, Agent Tesla, LokiBot, Zeus and Atmos are all designed to provide a core information stealing capability. More specifically, these tools are designed to steal usernames, passwords and other valuable credentials stored on an infected computer. These tools are widely available on underground forums, require minimal technical expertise to set up and are easy to deploy. Once infected, compromised systems transfer stolen information back to SilverTerrier actors using common internet protocols, such as Simple Mail Transfer Protocol, File Transfer Protocol or Hypertext Transfer Protocol – SMTP, FTP and HTTP, respectively. As a direct result, it's difficult to block the transfer of data with edge devices as these protocols blend in with normal activity on most networks.

Analyzing their use of these nine malware families, Nigerian actors are currently producing an average of 840 unique samples of malware per month (see Figure 2). This represents a 17 percent increase over the past year.

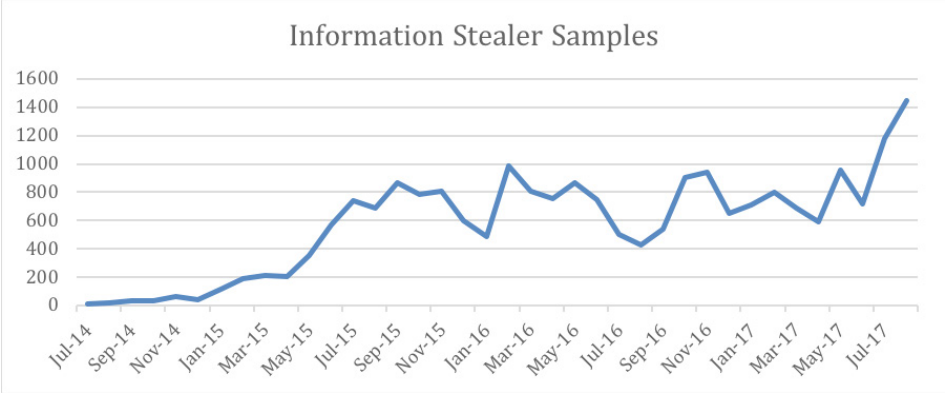

Figure 2 + Information stealer samples from July 2014 through July 2017

Though this growth is impressive, it is also misleading: each malware family's contribution to the total varies greatly. By exploring the individual contribution of each family in more detail, it becomes possible to illuminate tools that are gaining popularity, those maintaining steady use and those that have fallen out of favor.

Pony, LokiBot and Agent Tesla have emerged as the most popular information stealers in 2017. Pony is a fairly common malware family that has existed in various forms since 2012, with our first indications of Nigerian use occurring in August 2014. Since then, it has grown in popularity, reaching a peak of 858 samples in August 2017. Conversely, LokiBot and Agent Tesla are new malware tools. These two families have demonstrated steady growth over the past year, and we anticipate they will continue to climb in popularity and deployment over the next year (see Figure 3).

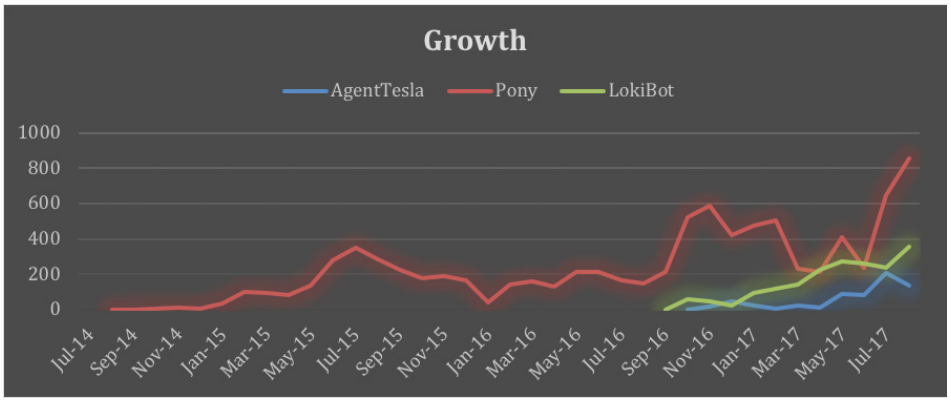

Figure 3 + Growth of Agent Tesla, Pony and LokiBot from July 2014 through July 2017

Predator Pain and ISR Stealer are established and well-maintained tools that have received a number of upgrades over the years. Although both reached their peak between 2015 and 2016, they maintain a steady following of users. The result can be seen in a constant flow of 20 samples per month of ISR Stealer and roughly 70 samples per month of Predator Pain (see Figure 4).

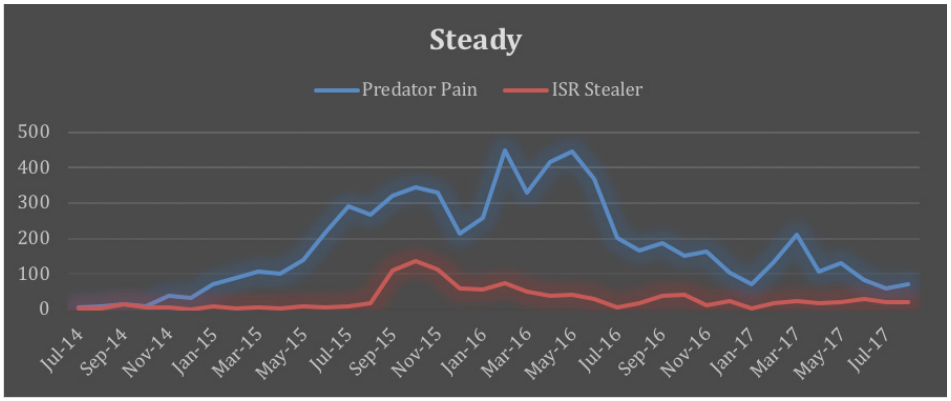

Figure 4 + Continued use of Predator Pain and ISR Stealer from July 2014 through July 2017

Conversely, our data also shows that four malware families have fallen out of favor. KeyBase, ISpySoftware and Zeus all experienced peak periods between May 2015 and November 2016. On the other hand, Atmos maintained a small but never substantial following. Of the four, KeyBase stands out due to its rapid rise in popularity, with a peak deployment of 160 samples per month and usage by 46 separate SilverTerrier actors, followed by a fairly rapid decline. Despite individual successes at various times, all four malware families have since declined in popularity to a rate of fewer than 10 samples per month in the three-month period from June to August 2017 (see Figure 5).

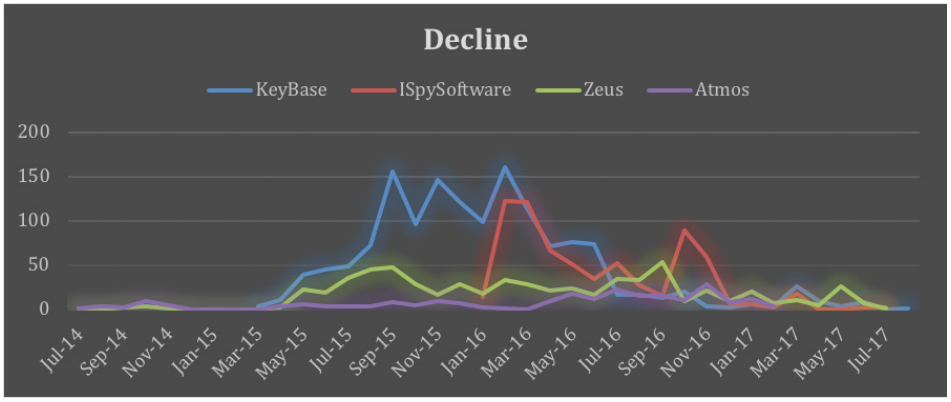

Figure 5 + Decline of KeyBase, ISpySoftware and Zeus from July 2014 through July 2017

Remote Administration Tools

NetWire, DarkComet, NanoCore, LuminosityLink, Remcos and Imminent Monitor are all designed to provide remote access to compromised systems. Although specific capabilities vary, many of these tools can capture keystrokes, monitor web cameras, access network resources and provide remote desktop connections. These tools are widely available on the internet, and not just on underground forums. Instead, public websites, such as Nanocore[.]io, Luminosity[.]link and DarkComet[.]net, provide cybercriminals with a means to purchase the tools as well as seek technical support and advice on how to configure and deploy the capabilities.

As the capabilities of RATs far exceed those of traditional information stealers, these tools require greater technical expertise to employ and more substantial infrastructure to control. Additionally, while information stealers transfer data periodically to command-and-control, or C2, servers that actors can check at a time of their choosing, RATs are more complex, requiring interaction with an adversary to be of value. Given this requirement, SilverTerrier actors often rely on Dynamic DNS and virtual private servers to provide a layer of obfuscation to protect their identities.

Unit 42 analyzed the use of these six malware families and found that Nigerian actors are currently producing an average of 146 unique samples of malware per month (see Figure 6). This represents a 49 percent increase over the past year. Although the monthly sample rate is a fraction of what we observe with information stealers, the annual growth rate is far more substantial. We are currently tracking 40 SilverTerrier actors who have already demonstrated the technical ability to employ these tools, and we anticipate these numbers will continue to rise sharply over the next year.

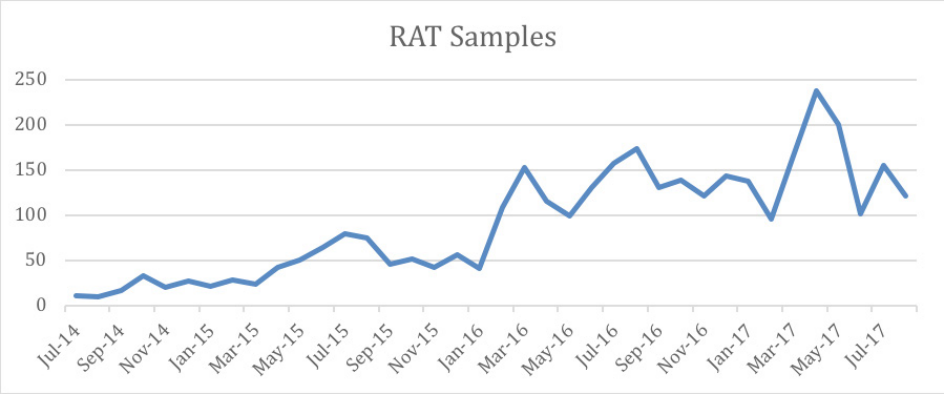

Figure 6 + RAT samples from July 2014 through July 2017

With respect to growth, NetWire, DarkComet and NanoCore stand out from their peers. Although none of these malware families are new, our data shows that NetWire and DarkComet both broke from a pattern of steady use and began to demonstrate greater adoption beginning in early 2017. In particular, NanoCore represents a fascinating case. This malware family began to demonstrate growth in January 2016 before reaching a peak in April 2017 with just over 100 samples. However, that same month, it was reported that the author behind NanoCore was arrested by the FBI, and since then,

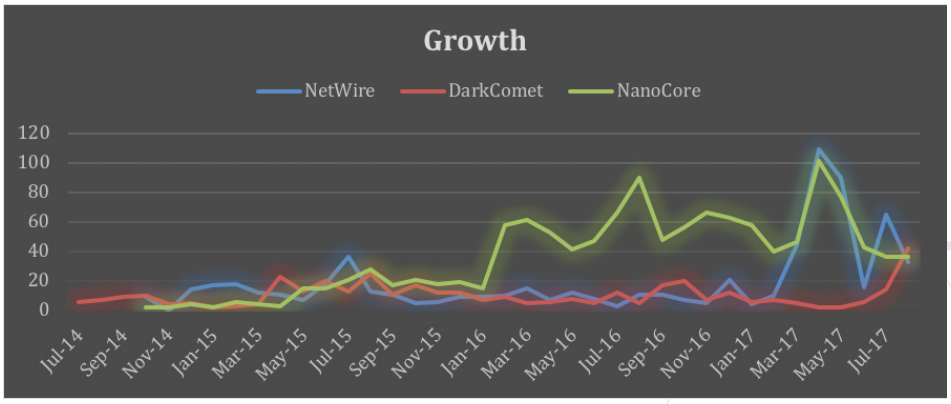

Figure 7 + Growth of NetWire, DarkComet and NanoCore from July 2014 through July 2017

we have observed a reduction – but not a complete decline – in its use. Despite this development, at the end of August 2017, SilverTerrier actors continued to produce more than 30 samples per month of each of these malware families (see Figure 7).

This brings us to the last three tools: LuminosityLink, Remcos and Imminent Monitor. Of the three, Imminent Monitor is the oldest and most established RAT, dating back to early 2013. LuminosityLink was released more recently in May 2015, and Remcos was first seen in June 2016. What is most interesting about these release dates is that, in both cases, SilverTerrier actors demonstrated an early ability to produce samples of these new tools. This provides unique insights into the technical proficiency of certain actors as well as their ability to gain access to new tools as they are released. However, as quickly as actors can adopt new tools, they can also abandon them. As of August 2017, all three of these tools have declined in popularity to a rate of fewer than 10 samples per month (see Figure 8).

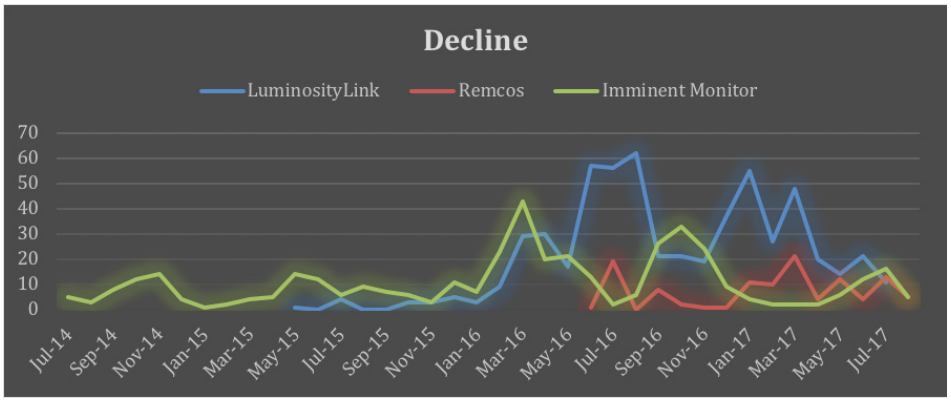

Figure 8 + Decline of LuminosityLink, Remcos and Imminent Monitor from July 2014 through July 2017

Malware Deployment Trends

SilverTerrier actors continue to refine and adjust their techniques for deploying malware consistent with their respective levels of experience. In the past year, we have identified 7,100 samples of malware associated with more than 181,000 attacks. This wealth of information continues to bolster informative analysis concerning malware distribution and C2 domains.

Malware Distribution

As these actors transition from their renowned email scams to the use of malware for financial gain, they have learned to scope the sizes of their target audiences. When using email scams, SilverTerrier actors preferred to use large target audiences, which maximized the likelihood of success with very little risk. However, nominal as it may be, there is a cost associated with generating new malware samples in terms of currency as well as time and energy required to establish C2 infrastructure. As a result, the majority of SilverTerrier actors continue to limit their target audiences in hopes of reducing the exposure of their malware to antivirus programs.

Our data shows 84 percent of the malware samples were observed in fewer than 20 attacks against our customers. Moreover, 92 percent of samples were sent to 50 recipients or fewer (see Figure 9). These numbers are on par with findings from previous years and remain significant as they demonstrate a consistent trend among all SilverTerrier actors to tailor their malware delivery to focused target sets.

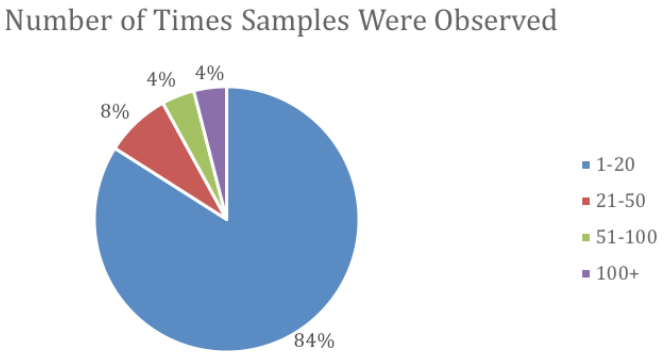

Figure 9 + Number of times malware samples were observed

In stark contrast, these actors are less than discriminating when it comes to the industries they target. Across our customer base, the high technology and higher education sectors continue to serve as the top two target areas, consistent with previous years. At the same time, attacks against the wholesale, transportation and telecommunication sectors have climbed substantially over the past year, securing positions three through five, respectively (see Figure 10). Regardless of this short list, it is important to note that we continue to witness attacks against every sector we track.

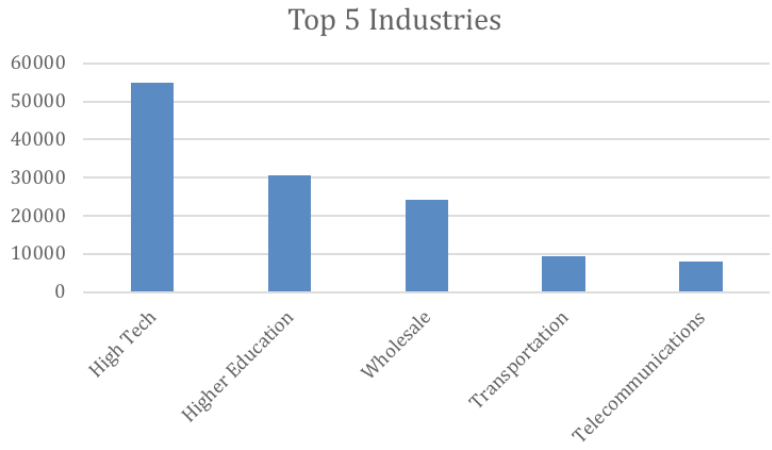

Figure 10 + Top five targeted industries

C2 Domains

To support the rapid growth and pace of malware distribution efforts, SilverTerrier actors are in constant need of domains to serve as C2 nodes. This drives a largely cyclical process in which an actor registers a domain name and allows it to sit for a period of time, potentially improving the domain's reputation. The domain is then weaponized to support malware schemes and, eventually, identified and blacklisted

by antivirus vendors and domain registrars. When this occurs, the actor simply moves on to the next domain on his or her list and continues the process.

Unit 42 tracks roughly 300 SilverTerrier actors who have registered a combined 11,600 domains over the past five years. These domains range in status from newly registered to suspended as well as to those that have now expired but serve to provide historical context surrounding an actor's activity. These domains also vary greatly in their usage. For example, some actors only register domains with the intent of supporting their malicious activities. However, it would be false to assume all actors follow this model. Instead, a considerable number of actors run legitimate businesses and simply use malware to supplement their income. In these cases, it becomes necessary to evaluate domains based on their individual merits to determine whether they serve benign or malicious purposes.

Across our data set, 19.3 percent of the 11,600 domains have been directly liked to malware activity. Another 6.6 percent have been associated with fraudulent activities, such as fake banking and shipping websites, distribution of spam, and other illicit activities. Additionally, 2.3 percent of domains provided email services that were used as mechanisms to deliver malware to victims. Combining all three – that is, malware activity, fraudulent activity and malicious email services – and accounting for the fact that some domains served a dual purpose, a total of 27.6 percent of domains registered by SilverTerrier actors have been linked to malicious activity.

Conversely, our analysis also reveals that a much smaller subset (1.2%) of the domains were registered to support legitimate business functions. Subsequently, there is also the remaining 71.2 percent of domains for which there is no firm evidence to support either legitimate or malicious use. Yet, although it is ultimately challenging to prove intent, the association of a domain to a SilverTerrier actor combined with analysis of domain names and registration details often provides valuable indicators. Following this approach, we assess that the vast majority of these domains were registered by actors with the intent of supporting illicit activity. To illustrate this point, consider the registration details for the domains us-army-mil[.]us and shell-ae[.]com (see Figure 11).

Attribute	Value
WHOIS Server	whois.nic.us
Registrar	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Email	lovethchukwuezi@outlook.com (registrant, admin, billing, tech)
Name	loveth chukwuezi (registrant, admin, billing, tech)
Organization	N/A (registrant, admin, billing, tech)
Street	no 10 mcc (registrant, admin, billing, tech)
City	owerri (registrant, admin, billing, tech)
State	Imc (registrant, admin, billing, tech)
Postal	23461 (registrant, admin, billing, tech)
Country	NIGERIA (registrant, admin, billing, tech)
Phone	2348056622055 (registrant, admin, billing, tech)

Attribute	Value
WHOIS Server	whois.namesilo.com
Registrar	NAMESILO, LLC
Email	wirelord1990@gmail.com (registrant, admin, tech)
Name	wire lord (registrant, admin, tech)
Organization	
Street	plot 101 world bank housing estate owerri (registrant, admin, tech)
City	owerri (registrant, admin, tech)
State	imo (registrant, admin, tech)
Postal	234 (registrant, admin, tech)
Country	NIGERIA (registrant, admin, tech)
Phone	23408096392798 (registrant, admin, tech)

Figure 11 + Registration details for us-army.mil[.]us and shell-ae[.]com

In both examples, the domain names themselves can be used to provide indicators as to the actor's intent. To that end, it is very unlikely that the United States government or Shell, a global energy company, would commission SilverTerrier actors to develop domains that impersonate their own legitimate websites and services. Moreover, the second example further demonstrates the value of individual registration details. Understanding that Nigerian actors use the term "Wire Wire" to describe BEC schemes, it is possible to draw conclusions about a domain registered under the name "Wire Lord" with an address referencing a "World Bank Housing Estate."

Unfortunately, these two cases are by no means unique. It is fairly common for Nigerian actors to establish domains with slight misspellings that impersonate legitimate organizations they intend to target, a practice sometimes referred to as "typosquatting." Although this is still the most prevalent technique for actors employing information stealers, it does not apply to all malware families. Given the requirements of RATs, we also observed growth in the adoption of Dynamic DNS services.

DDNS complicates the ability to identify actors, but we have found that many of these hurdles are surmountable as next-generation firewall, or NGFW, technology provides a wealth of technical indicators that can be applied to empower advanced threat analytics. For example, doncjpd.ddns[.]net and puffydon.ddns[.]net both serve as C2 domains for NetWire. Because they are sponsored by a free DDNS provider, no additional ownership information is publicly available. Despite this constraint, NGFW analysis can be leveraged to illuminate unique and rare behaviors shared between individual malware samples. In practice, these details enable correlation with other domains registered to the same email address: **cj_puffy2004@yahoo.com**. Using advanced analytic resources, it then becomes possible to quickly enumerate more than 75 additional domains associated with just one actor.

Who Are They?

Exploring SilverTerrier actors in more detail, we've confirmed a set of common characteristics that continue to resonate and hold true as well as, interestingly, buck traditional stereotypes associated with cybercriminals. For example, these actors take little to no care to remain anonymous. The credentials they use to register their malware infrastructure are easily associated with their public social media accounts on Google®, Facebook®, MySpace®, Instagram®, and various dating and blogging sites. Despite the passage of laws prohibiting fraud, scams and other illicit activity, the culture in Nigeria remains permissive of cybercrime, and widespread enforcement of the laws has yet to be observed.

Although social media accounts should never be considered definitive sources of information, they can still provide significant insights into the demographics associated with these actors. Specifically, the accounts reveal that SilverTerrier actors are mostly mature adults, not children or teenagers. They range in age from their 20s to 40s with few exceptions, and the vast majority are estimated to be in their 30s. Many of the actors are married with children and have held a variety of legitimate jobs throughout their careers. Further, these actors are also allegedly educated, with more than 55 percent of attributed actors listing colleges and universities on their profiles and one actor claiming to be a lecturer at a local university.

It is also important to note that, when it comes to career choice and motivation, each SilverTerrier actor is unique and falls across a diverse spectrum. Among the list of actors are those who pursue cybercrime as a full-time activity; those who provide enabling activities, such as web hosting or domain resale; and those who own a mix of legitimate and fraudulent domains. With the latter, we assess that many such actors view cybercrime as a means to supplement their legitimate income, as they most often maintain employment with organizations in the technology, education, media or music industries.

At the same time, a second consideration that should not be discounted is that each actor pursues cybercrime only for a limited time period of their choosing. For example, our data set contains more than 300 actors, but it should not be inferred that each actor is active every month. We have observed that, between early 2015 and early 2016, the number of actors active in a given month tripled over the course of a year, from roughly 30 to 100 actors. Since early 2016, the number of active actors has remained relatively steady, hovering between 75 and 117 over the past year (see Figure 12). These metrics demonstrate a degree of equilibrium among the SilverTerrier population, with new actors joining these malicious activities at a rate consistent with those departing cybercrime. Often perceived as a positive situation, this state of equilibrium also raises concerns as it suggests the actors are becoming more proficient due to growth in malware production and observed attacks over the same time period.

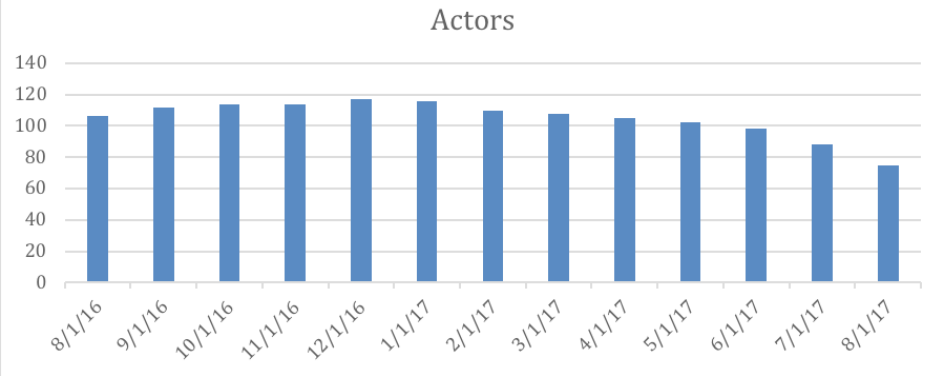

Figure 12 + Number of actors per month from August 2016 through August 2017

Shifting to their geographical dispersion, many SilverTerrier actors are situated in and around the major cities of Nigeria. Nevertheless, a small contingent of Nigerian actors has been identified outside Nigeria in various locations across the globe. The list of locations has expanded over the past year as actors have been identified living abroad in the United States, United Kingdom, Malaysia, Turkey and other African countries.

Given this dispersion, SilverTerrier actors continue to demonstrate growth in their organized structure with minimal degrees of social separation. Although the number of actors continues to fluctuate, these actors remain in similar social circles based on the universities they attended, social network connections for the tools they use or cities in which they live. As a result, social media platforms, such as Facebook and Google+®, serve as excellent tools to support elementary-level link analysis between actors. In fact, link analysis proves remarkably successful when applied

to identify new or suspected threat actors and facilitators. For example, consider a scenario in which you learn that three known threat actors all share a common friend. In reviewing that friend's profile, you observe that his profile picture flaunts foreign currency, his job title is "CEO of Self-Employed," and he happens to be a member of several online technology and hacking clubs. Alone, none of these bits of information are conclusive, but when combined and paired with an association with known SilverTerrier actors, such an individual definitely stands out (see Figure 13). Employing this technique over the past year, Unit 42 has successfully linked many of these individuals to previously unattributed samples of malware.

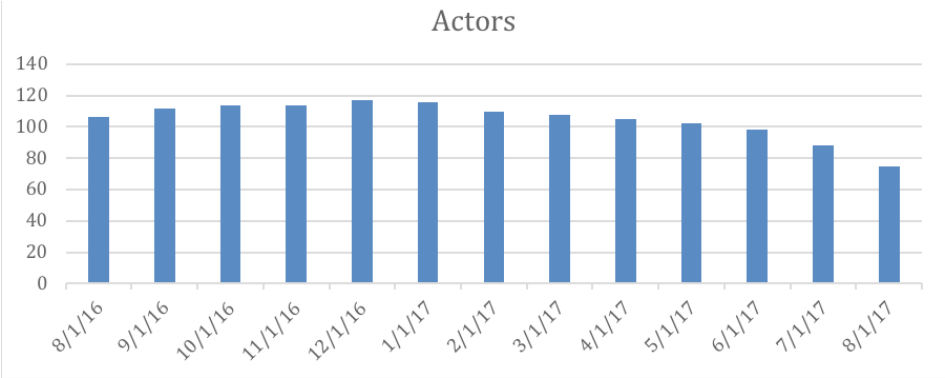

Figure 13 + Using social media to identify suspected cyber actors

In addition to enabling link analysis, these social media platforms also provide insights into public groups dedicated to online cybercrime. For example, searching for the terms "Wire Wire" or "Wire Transfer" on social media platforms often reveals several groups associated with cybercrime and further provides a means to identify suspected participants. The group "WIRE WIRE.COM" on Facebook serves as a prime example (see Figure 14). Using this public group, members have exchanged contact information and solicited help with their illegal activities.

Figure 14 + WIRE WIRE.COM Facebook Group

This group also serves as a key resource for cybersecurity analysts seeking to identify leadership roles and relationships between actors. Specifically, new members requesting access to this group need to be sponsored by existing members. This results in the membership page for the group containing a list of suspected cybercriminals and the names of those who sponsored them for access, as well as the date they joined the group (see Figure 15).

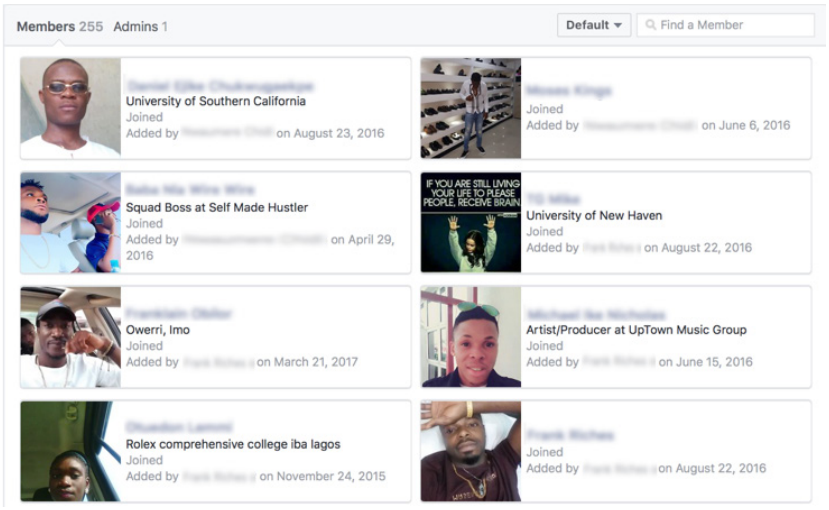

Figure 15 + **WIRE WIRE.COM membership details**

Combining the wealth of publicly available information with data from Palo Alto Networks malware repositories continues to drive various degrees of attribution analysis. It also promotes an enhanced understanding of the interconnections between actors, suspects, tools and organizations. This analysis is applied to enable predictive analysis with the goal of enhancing the preventive capabilities of our platform.

Attribution

Attribution is a complex concept that often evokes a wide range of perceptions depending on the audience to which it is presented. To consumers of cybersecurity reports, the term is commonly viewed in a positive light as it is used to link nefarious characters directly to the crimes they commit. On the other hand, from a strictly business standpoint within the cybersecurity industry, the term is often viewed through a more ambivalent lens. This distinction is due to attribution efforts often requiring tremendous analytic resources without a guaranteed return on investment. This results in cybersecurity organizations focusing their sparse investigative resources against high-priority threats. Though pragmatic in its approach, this line of thinking has simultaneously advanced yet constrained the industry.

The world has undoubtedly witnessed iterative advancements over the past decade as stories describing cyber intrusions have cemented positions as trending, front-page news. Concurrently, reports produced by cybersecurity organizations and private researchers have expanded to a point where they effectively complement and inform efforts historically performed solely by government and law enforcement organizations. However, despite this positive trend, many of these attribution efforts

remain scoped and constrained to data sets with no more than a handful of criminals, a couple of malware samples and a few dozen other indicators. Simply put, the efforts are scoped consistent with the analytic resources that can be brought to bear against a specific data set. By comparison, the SilverTerrier data set has grown to become multiple orders of magnitude greater. With more than 300 actors, 11,600 domains, 30,000 samples of malware and details surrounding roughly 500,000 attacks, the challenge with using a data set of this size quickly becomes a question of scale. For the cybersecurity industry at large, the ability to scale attribution efforts to accommodate ever-expanding data sets while minimizing resources and maximizing results remains a nascent concept.

In evaluating the success associated with this analytic effort, we believe advancements in data-visualization techniques, the wealth of data produced by NGFW products, and "big data" analytics can be combined to achieve valuable attribution insights that encompass the breadth and depth associated with large data sets. To that end, we recognize there are many levels of attribution, each delivering different degrees of value depending on the target audience. For example, the highest levels of attribution link cyber activities directly to individuals and their social media accounts, physical addresses, and other descriptive characteristics (see Figure 16). These details are often desirable as they shed light on the motivations, relationships, experiences and capabilities of an individual actor, but this level of analysis is also considered the most resource-intensive.

Figure 16 + **Example of high-level attribution**

On the other end of the spectrum are lower levels of attribution, which are often discounted and overlooked but can augment network defense when applied effectively. Consider, for a moment, if your network security could not only identify malware but also provide insight into the actor group responsible. From a research standpoint, the resources required to achieve this result are minimal, and easy to automate and develop into scalable approaches. Simply identifying malware C2 domains and correlating patterns associated with domain registration details can provide these low levels of attribution (see Figure 17). As such, we believe that, for minimal cost, these efforts provide Palo Alto Networks customers with greater visibility into the threats targeting their networks as well as enable customers to tailor their investigative resources accordingly.

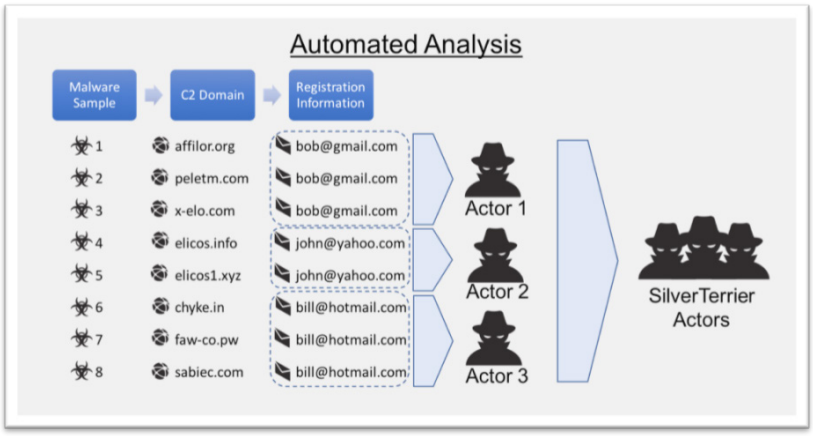

Figure 17 + **Example of low-level attribution**

In between these two lies a fascinating range of capabilities that can expand upon low-level attribution and provide immensely valuable information for network defenders at minimal cost (see Figure 18). When evaluating how to scale attribution efforts for large data sets, this becomes the ideal case. For example, low-level attribution efforts can easily be augmented through the automated use of resources such as PassiveTotal™ or DomainTools®, which can be leveraged to pivot through and identify a complete list of domains associated with a specific actor. Recognizing that each cybersecurity company only observes attacks against its own customer base, this complete list of domains can then be compared across the industry to further enrich the data set. Combined, this largely automated approach produces significant results, building a foundational picture of a cyber adversary and, more importantly, a foundation for predictive analysis.

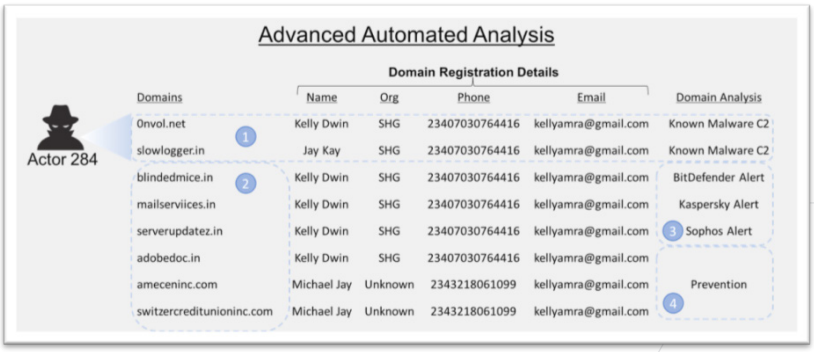

Figure 18 + **Example of medium-level attribution**

Using Figure 18 as an exemplar, we first identify the domains slowlogger[.]in and 0nvol[.]net as being directly linked to known malware samples within Palo Alto Networks malware repository. Using the registration details associated with these two domains as a starting point for enumeration, we use PassiveTotal to identify six previously unknown domains registered to the same actor. These new domains help form a profile of the actor by establishing an association between three names, one organization, two phone numbers and a single email address. If needed, we can apply these details later to support higher levels of attribution analysis. Next, we evaluate the domains across the industry to reveal that other cybersecurity organizations have already flagged three as malicious. Finally, in the last step, we manually analyze the remaining three domains in conjunction with the totality of the actor's activity. As it applies to this example, the actor is associated with eight domains, five of which have been attributed to malicious activity, while the remaining three appear to impersonate a technology company, a supply chain management organization and a credit union, respectively.

Armed with this powerful perspective, network administrators can begin to tailor their defensive capabilities to focus on prevention, adopting a proactive posture against anticipated threats. Applying this concept to the SilverTerrier data set as a whole, Unit 42 has successfully scaled this level of attribution and analysis against an expanding data set using minimal resources, with tremendous gains. These techniques continue to enable Palo Alto Networks to identify suspicious domains and put preventive measures in place prior to the first samples of malware reaching our security products.

Conclusion

Key Takeaways

- Nigerian cyber actors remain a formidable threat to businesses worldwide, demonstrating a 45 percent increase in attacks recorded from August 2016 through August 2017.
- These actors are educated adults ranging in age from their 20s to 40s. Many participate in cybercrime as a means to supplement legitimate employment, and most actors leverage social media platforms as tools to promote organization and collaboration.
- Information stealing malware families remain in common use, with SilverTerrier actors producing an average of 840 samples per month. This represents a 17 percent year-over-year increase, with Agent Tesla, LokiBot and Pony standing out as the most popular tools in the category.
- SilverTerrier actors have begun to incorporate RATs into their criminal activities at a significant rate. Our data shows these actors can produce an average rate of 146 samples per month. This represents a 49 percent increase over previous years, with the three most popular tools being DarkComet, NetWire and NanoCore.
- There is tremendous value to be gained from conducting advanced automated analysis of cybercriminals employing commodity malware. Palo Alto Networks continues to employ and refine these methods across expansive data sets to identify, track and prevent attacks against our customers.

Protection and Mitigation

Customers of Palo Alto Networks are protected from this threat in both of the following ways:

1. Threat Prevention flags C2 domains used by these actors as malicious.
2. WildFire® cloud-based threat analysis service and Traps™ advanced endpoint protection accurately identify samples associated with these malware families.

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

- PredatorPain
- BilalStealer (ISR Stealer)
- KeyBase
- ISpySoftware
- Pony
- AgentTesla
- LokiBot
- Zeus
- Atmos
- NetWire
- DarkComet
- NanoCore
- LuminosityLink
- Remcos
- ImminentMonitor
- SilverTerrier

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

unit42

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com