Introduction

Welcome to this Hewlett Packard Enterprise (HPE) Security Research analyst report. In this report, we cover operational security (OPSEC) practices employed by cybercriminals as observed by our researchers during the regular collection and analysis of threat intelligence in the first half of 2016. The report begins with an introduction into operational security and follows with its application to cybercriminal operations. We highlight cybercriminal OPSEC practices used to hide their real identities, as well as their mistakes. We cover criminal infrastructure, operational processes, malicious code, and – for the first time – the quality of their passwords recovered from various cybercriminal operations in comparison to the quality of passwords used by legitimate users.

About Hewlett Packard Enterprise Security Research

HPE Security Research conducts innovative research in multiple focus areas, delivering security intelligence across the portfolio of HPE security products. In addition, our published research provides vendor-agnostic insight and information freely to the public and private security ecosystems.

HPE Security Research brings together data and research to produce a detailed picture of both sides of the security coin—the state of the vulnerabilities and threats composing the attack surface, and the ways adversaries exploit those weaknesses to compromise targets. Our continuing analysis of threat actors and the methods they employ guides defenders to better assess risk and choose appropriate controls and protections.

Our methodology

To document and analyze cybercriminal OPSEC, this report draws on research from HPE’s Security Research teams and previous research conducted by several other organizations and individuals. The report can be used by security practitioners to raise awareness about the importance of OPSEC and its application in the cybercriminal underground. The report speaks specifically to investigations conducted during the first half of 2016. Links in this report were active as of 07/2016.
# Table of contents

1 Introduction .......................................................................................................................................... 1  

2 Background .......................................................................................................................................... 1  
2.1 Five stage OPSEC process................................................................................................................... 1  
  2.1.1 Identify critical information ........................................................................................................ 2  
  2.1.2 Analyze the threat ..................................................................................................................... 2  
  2.1.3 Analyze the vulnerabilities ....................................................................................................... 2  
  2.1.4 Assess the risks ....................................................................................................................... 3  
  2.1.5 Apply the countermeasures .................................................................................................... 3  

3 Criminal OPSEC analysis ................................................................................................................... 4  
3.1 Cyber-criminal OPSEC practices....................................................................................................... 4  
  3.1.1 Unsuspecting partners ............................................................................................................. 6  
3.2 Cyber-criminal infrastructure and services ...................................................................................... 7  
3.3 Common OPSEC infrastructure mechanisms used by malicious actors.......................................... 8  
  3.3.1 IP address hiding mechanisms .............................................................................................. 8  
  3.3.2 Virtual Private Networks (VPN) ............................................................................................ 8  
  3.3.3 Anonymity networks .............................................................................................................. 9  
  3.3.4 Virtual Private Servers (VPS) / Bulletproof hosting .............................................................. 10  
  3.3.5 Hop points / Compromised servers ....................................................................................... 10  
3.4 Cyber-criminal password quality ....................................................................................................... 10  
3.5 Malicious code OPSEC .................................................................................................................... 15  
3.6 OPSEC - Attribution and Advanced Persistent Threat (APT) actors ............................................. 16  

4 Conclusion ......................................................................................................................................... 18
1 Introduction

Operational security (OPSEC) is an important component of cybercriminal operations. Faced with the ever increasing focus and capabilities of law enforcement agencies, criminals must take measures to hide their real identities while continuing to operate in the cyber underground. Without strong OPSEC, criminal operators are quickly discovered, as we see almost on a weekly basis in various reports documenting police operations and arrests\(^1\).

Security researchers also have a requirement for operational security. As cybercriminals increase their skills, security researchers need to take all precautions in order to keep their underground cover identities safe. This allows them to continue tracking cybercriminal operations in order to protect their own users and resources, detect intrusions, share threat intelligence and cooperate with law enforcement agencies around the world while preserving anonymity to maintain their own physical security.

Since cybercriminals, security researchers and law enforcement agents all conduct covert cyber operations, it is not a surprise that some of the best OPSEC practices can be applied to all these actors in cyber space.

2 Background

OPSEC is not a new discipline having been practiced in many military operations with its first systematic mention as a process during the Vietnam War operations\(^2\).

The process of identifying critical information and analyzing friendly actions attendant to military operations and other activities in order to:

- Identify those actions that can be observed by adversary intelligence systems.
- Determine indicators and vulnerabilities that adversary intelligence systems might obtain to be able to interpret or piece together to derive critical information in time to use against U.S. and/or friendly missions and poses an unacceptable risk.
- Select and execute measures that eliminate the risk to friendly actions and operations or reduce to an acceptable level.

2.1 Five stage OPSEC process

It is commonly understood that OPSEC is a process consisting of five stages:

\(^1\)http://fortune.com/2016/07/17/taiwan-atm-cyber-robbery-arrest/

\(^2\)http://www.opsecprofessionals.org/origin.html
2.1.1 Identify critical information

Critical information is defined as specific facts about friendly intentions, capabilities, and activities fundamentally needed by adversaries to plan and act effectively. If Critical Information is obtained, the adversary would be able to cause friendly mission failure or other mission degradation.

Threat actors need to identify the critical information that allows their enemies to predict their real identities and actions. Protecting personal identities and staying anonymous is the main goal of the cyber(criminal) OPSEC.

2.1.2 Analyze the threat

Once critical information is identified, the next step is to determine the individuals or groups that represent a threat to that information. There may be more than one adversary, and different information may be targeted by different groups. In this stage, the capabilities, use for the information, determination and resources must also be analyzed.

For cybercriminals, the main threats are law enforcement agencies, the U.S. Secret Service and, to an extent, security researchers. In each case, these agencies attempt to track cybercriminals and discover their real life identities in order to prosecute them and disable their actions by putting them into corrective facilities for long periods.

2.1.3 Analyze the vulnerabilities

In this phase, the OPSEC practitioner “thinks like a wolf” - that is, they view their organization from an adversary’s perspective. The organization’s vulnerabilities must be thoroughly explored, especially in terms of physical safeguards, network/electronic safeguards and personnel training.

This equally applies to cyber OPSEC. For criminals, it means examining their own organization, processes and infrastructure to find potential weaknesses that can be exploited by their adversaries (e.g. law enforcement). Just like a legitimate enterprise, cybercriminals use third-party software and services that may have vulnerabilities requiring significant resources for regular patching and system maintenance, which is often neglected for higher priority tasks.
To achieve its goal, cybercriminal OPSEC needs to strike a fine balance between keeping the operation covert and allowing the operation to continue without a slowdown.

### 2.1.4 Assess the risks

Every vulnerability directly relates to a specific threat. At this point, each vulnerability is assigned a risk level. This is an unmitigated risk level, meaning that any corrective factors are not included in the analysis.

![Risk assessment matrix](image)

**Figure 2** Risk assessment matrix

### 2.1.5 Apply the countermeasures

Beginning with high-risk vulnerabilities, a mitigation plan is put in place with the most important element being to develop a plan to lower or eliminate the risk, or remove the threat's access to the resource.

Countermeasures must be continuously monitored to ensure they remain effective and relevant. Threats change, as do the methods of attack or the vulnerabilities affecting an organization. It's important to review countermeasures to ensure they are protecting critical information against the right threats at the required time.
Applying countermeasures is usually the only well-documented step of criminal OPSEC and is actually considered to constitute good OPSEC practice in general in the cyber underground world. The most well-known document describing countermeasure application for cyber OPSEC is the “Jolly Roger’s Security Guide for Beginners\(^3\), which is widely quoted in underground and deep web forums.

3 Criminal OPSEC analysis

3.1 Cyber-criminal OPSEC practices

OPSEC of criminal actors is somewhat similar to the OPSEC of security researchers tracking those criminals with best practices versus actual practices. This section contains a few examples of what criminals say in regards to securing themselves and the relationship of their countermeasures to what we have actually observed.

HPE Security Research takes every opportunity to grab database (DB) dumps of criminal forums in order to analyze for intelligence purposes. Within the dumps are IP addresses, usernames, email addresses, plain text and hashed passwords, and – sometimes – even conversations via private messaging on the forums. On many forums, criminals were observed engaging in conversations about VPN services and choosing one over another due to logging. In reality, our researchers found a mix of good OPSEC practices and clear OPSEC failures.

There are a variety of forums with some being more “lightweight” than others in regards to criminal activities. Typically, the heavyweight forums are engaged in criminal activities such as carding, bot selling and trading, selling user information, and other cybercriminal activity. The lightweight ones are more concerned with sharing knowledge and tools without actually attempting to disclose or sell stolen information.

Analysis of the exposed IP addresses from recovered databases revealed that a good number of users log in from their home IP addresses. This was observed to varying degrees and was dependent on the forum’s type and activities. The lightweight forums have more users logging in from home IP addresses due to the fact they may feel safer or they are just starting the life of a cybercriminal and have yet to figure out how to protect themselves. Many users on the lightweight forums will also use Tor over any kind of VPN.

On the other hand, users on the heavyweight forums are more likely to use a VPN or a Virtual Private Server (VPS) to hide their home IP addresses. Frequent switching of IP addresses used to be common practice, but after a few account compromises cybercriminals now try to keep to a static IP so that the forum administrators can tell if someone else is logging into their accounts. More recently, criminals started to use bulletproof hosted VPS services to hide behind; ones they trust not to leak their information. Surprisingly, a lot of users in Russia have been observed logging into forums from their home IP rather than using a VPN. They likely feel they are protected by residing in Russia.

Other observations include evidence of bad security practices and sloppy forum usage. Some users will always try to log in from VPN and then one time log in from their home IP. Is this intentional or did they forget to start their VPN connection?

Username and email address reuse are also a common cybercriminal practice. This is done for a number of reasons including laziness, and reputation building. Managing multiple email addresses every day, or even every hour, can be time consuming, as is managing multiple addresses and usernames. In the criminal world reputation is everything, requiring the cybercriminal to protect their identity to compete in business. Building a single well-known identity is much easier – and less time consuming – than working on multiple identities to achieve a reputable status.

3 https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/
This is not to say that criminals don't use multiple email addresses; they do, but often for different business reasons. When it comes to identity and/or usernames, they will try to keep it to just one. If for some reason they need a different username, they will usually try to get someone they know to vouch for them, thus retaining their well-crafted reputation and applying it to the new username.

When it comes to identifying criminals on forums, the reuse of credentials is a big help to the research community. It is often possible to identify the same person across multiple forums based on usernames and email addresses. Many times, in the DB dumps, the same usernames and email addresses are tied to each other. Other times, a known username will be tied to a different email address. This typically means that same cybercriminal tied to the username has chosen a different email address for some reason – possibly because it is a forum the criminal does not yet fully trust.

Personal history is another important factor for discovering the criminal's real identity. Everyone starts from somewhere, and criminals will start with one username. As they learn and grow their reputation, they often use the same username, even after running their own botnets and committing various forms of fraud. This weakens their OPSEC as they were not as secure in the beginning as they eventually became. Looking at old domains used or postings on forums often reveals a clue to their true identity. Many cybercriminals do not think about hiding their registered domain WHOIS information, meaning the record may still contain their real name and home address.

Others have posted information such as what country they live in and what languages they speak so that they can try to relate to others on the forum. They will sometimes post an email address that is their personal email address without thinking that they are exposing themselves in this way or they will use their personal email address with their username without separating the two. Those that don't learn to separate their criminal life from their personal life expose much when researchers and law enforcement investigate them.

Forums themselves also provide a certain level of security for their users. Basic criminal forums and shops are hosted on virtual private servers (VPS) or custom servers and offer basic security. They usually use open source forum software such as Vbulletin or PHPBB3. They are hosted on the web where anyone using an internet search engine will be able to find them. Lately, there has been a push to host a number of criminal domains on Tor domains. This ensures that users never learn where the server is hosted thus protecting the forum to a certain degree. Another way of protecting forums is the use of the CloudFlare service. CloudFlare, normally used by legitimate sites as a content distribution network and as protection against certain types of attacks, is also being used by cybercriminals to protect forums and botnet panels.

The location of the host also plays into the security of the server. If it is hosted someplace where law-enforcement agencies can easily seize it, the forum is less secure and less trusted. Most criminal forums are hosted on bulletproof hosting services specifically set in a location where law enforcement either can't reach or has a very hard time getting to them. A number of criminal forums are hosted in Russia where non-Russian law enforcement agencies will have difficulty serving warrants.

A few of the really heavyweight Russian sites use an entirely different method in protecting themselves. They will use a client based certificate and an odd port number to hide themselves and make it almost impossible for law enforcement and/or security researchers to get on the forum to see what is going on.

Overall, the effective cybercriminal OPSEC countermeasures are:

- **Isolation** - only necessary communication to collaborators on a need-to-know basis
- **Compartmentalization** - never mix home and business; never work from home
- **Encryption** – for data in transit and at rest
- **Strong authentication** – use two factor authentication or client side certificates to authenticate
- **Anonymization** – Tor, reusable virtual machines which cannot be identified, access to public WiFi and anonymous 4g MiFi, Bitcoin payments
- **Alternate identities** - develop a believable online persona for different tasks; the longer the history the better
- **Patch vulnerabilities**
- **Healthy paranoia** – chances are law enforcement is looking for you, so be vigilant but do not let this block you
- **No bragging about your business**
- **Assume everyone is an enemy**
• Use bulletproof hosting
• Do not fall into a routine - vary your IP address and machine fingerprints; deceive others about who you are and where you are
• Do not look and act like a criminal - do not spend money to buy luxury items that would normally be beyond your means
• Properly manage images and social networks - remove image metadata, or, even better, do not post any images; do not use victim’s infrastructure to post to your personal social network accounts
• Guard your hardware - never leave it in your room; never take more devices on a trip than you actually need; mask your webcam and microphones; use screen privacy filters

On the other hand, common criminal OPSEC failures are:
• Contamination - mixing real and fake identities; for example using the real name as a username, using real email addresses, domains registered in the real name, use of home IP address for criminal operations
• Reuse of credentials - the higher the reuse the higher the risk of being discovered
• Weak passwords
• Forgetting basic OPSEC - connecting to the victim or C2 system with the real IP address by mistake
• Testing malware on their own computer, infecting it and becoming a part of a tracked botnet
• Leaving trails in malware to get public attention
• Bragging on social networks
• Following their own real personal accounts on social networks
• Leaving payment trails
• Leaving trails of activity in browser cache
• Collaborators exposing activities either through bad OPSEC or deliberately after cooperating with law enforcement agencies or otherwise

3.1.1 Unsuspecting partners

Organized crime actors often use “ordinary” people in their criminal enterprises. Most of these people have never been on a criminal forum or even know that they are in fact an essential part of a criminal operation. They can almost be considered victims looking for jobs on various job offer sites. As a part of their new “job” they do exactly what they are instructed to do, like registering a domain name using their personal details, writing a piece of a code, or helping out with the infrastructure for a bulletproof hosting company. For a researcher, this generates a lot of noise and most of the time leads to a research dead end.

Getting through the layers of the organized crime actor’s organization can consume a great deal of time before the person orchestrating the entire operation is exposed. The most effective way to get to the organizer is skip tracing and employing social engineering techniques to collect as many small pieces of evidence to get to the final picture.

In one case, a coder was hired through a head hunting website, hh.ru, to develop a framework. The framework was eventually used as a botnet panel. The coder was also asked to maintain the server and register a domain. This meant that all the information pointed to the coder and not to the organizer. The organizer of the criminal activity then used other criminal services to get as many bot infections connecting back to the botnet panel as they could. In the end the organizer gathered gigabytes of data while minimizing their electronic footprint.

It was possible to determine the real identity of the coder because of his poor OPSEC. This identification led to the misidentification of the coder as the mastermind behind the operation since all digital evidence pointed to him. In this case, the true organizational structure of the operation was revealed after employing social engineering techniques to get the real mastermind to explain his business model.
3.2 Cyber-criminal infrastructure and services

To accomplish anything on the Internet you must connect to it, which immediately exposes your operations. Though the Internet is vast, it is finite and the access-ramps to it are identifiable. Generally, there are three different infrastructure components that comprise the building blocks for any Internet presence. These are:

**Internet Protocol (IP) Address** – This is the fundamental building block of the Internet. Every device connected to the Internet must be able to communicate via either a public IP address or a private IP address that shares a public IP address via Network Address Translation (NAT).

**Fully Qualified Domain Names (FQDN)** – A FQDN is the human readable domain name that is translated to an IP address. FQDN is not necessarily essential to the work of a malicious actor, depending upon what they are trying to do. Using FQDN allows the actor to move to different IP addresses without having to change the rest of the kill chain. FQDN’s are also used to lend legitimacy to attack vectors. Second Level Domains (SLD’s), registered through domain registrars and directly under the various Top Level Domains (TLD’s) (i.e. .com, .net, us, org, etc...), may or may not be available due to the use of privacy services. The registered owner of an SLD is responsible for resolving all third level (and greater) domains.

**Email Address** – Like FQDN, an email address is not always required by a malicious actor. Email addresses can be easily spoofed if a reply is not required. Disposable emails can be employed by actors who need to get responses or send emails. Actors investing a little more time can acquire emails using false information.

Each of these components can be acquired by a bad actor using one of three methods:

**Legitimate** – Legitimate acquisition of these components has the actor going to a supplier of the desired infrastructure components to purchase them outright. “Legitimate” refers to the actor’s actions and not the reputation of the vendor.

**Fallacious** – Fallacious acquisition suggests that the actor acquires a service using false credentials or identification. A good example is the purchase of a Second Level Domain (SLD) from a domain registrar using false contact information. Fallacious acquisition is easier if the service does not require payment. However, criminal actors can, and do, acquire services requiring payment using false credentials. The payment itself may use legitimate means (prepaid cash cards, digital currencies, or other mechanisms).

**Criminal** – Criminal acquisition is any kind of theft of services, either by using stolen credit cards to buy legitimate services, or by hacking into a vulnerable network or server to use those resources without the legitimate owner’s approval.

Table 1 attempts to generally express the difficulty of accurately identifying a real person from the infrastructure item and the means by which it was acquired.

---

Table 1 | Ease of building block attribution based on the acquisition method of Building Blocks Based on Acquisition Method

<table>
<thead>
<tr>
<th></th>
<th>IP Address</th>
<th>SLD</th>
<th>FQDN</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legitimate</strong></td>
<td>Easy</td>
<td>Some Effort</td>
<td>Difficult</td>
<td>Easy</td>
</tr>
<tr>
<td><strong>Fallacious</strong></td>
<td>Some Effort</td>
<td>Difficult</td>
<td>Extremely Difficult</td>
<td>Difficult</td>
</tr>
<tr>
<td><strong>Criminal</strong></td>
<td>Extremely Difficult</td>
<td>Extremely Difficult</td>
<td>Extremely Difficult</td>
<td>Extremely Difficult</td>
</tr>
</tbody>
</table>

3.3 Common OPSEC infrastructure mechanisms used by malicious actors

Regardless of the method of acquisition, malicious actors use various mechanisms to further impede investigators' ability to determine the true identity of their on-ramp to the Internet. Remember, if an investigator can discover the actual IP address the actor is using to get onto the Internet then, depending upon who and where they are, they can either be prosecuted for their actions, or the nation that they are working for can be chastised diplomatically.

3.3.1 IP address hiding mechanisms

Actors attempt to hide their IP addresses using a variety of techniques. Many times they will stack several methods on top of each other. For example they may use a Virtual Private Network (VPN) connection to connect to another VPN and then further hide their connection by then joining the TOR or Riffle network. The task of ultimately properly identifying the “real” IP address of the actor may seem daunting, but dedicated researchers who are pursuing specific actors watch for slips in their OPSEC practices. The identity of more than one actor has been determined when their VPN connection quit unexpectedly and their real IP address was revealed as the software they were using reestablished a connection.

3.3.2 Virtual Private Networks (VPN)

A VPN allows someone to connect from an IP address into a private, encrypted network tunnel and have their traffic come out somewhere else with an IP address associated with the VPN provider’s network.

Figure 3 shows a small list of top-rated VPN providers that are readily available. The graphic shows the number of countries, servers and IP addresses available from each provider. These are commercial providers, but there are also a variety of free VPN networks as well.
3.3.3 Anonymity networks

The Onion Router (TOR) is the most well-known of networks based upon “onion encryption.” The concept and software supporting onion encryption was originally developed by the U.S. Navy for the express purpose of preserving the anonymity of its users. The original intent of the software was to allow for the safe communication of information from dissidents and others in oppressed countries in the interest of supporting freedom. Today, the TOR Project is its own entity and is supported by the Electronic Freedom Foundation (EFF).5

While TOR has some constraints, it is widely used by a variety of actors. Unfortunately these actors include not only dissidents in oppressed countries, but also purveyors of child pornography, sellers of illegal drugs and, more recently, extortionists collecting Bitcoins from victims whose files have been encrypted by ransomware.

Figure 3 Top-rated VPN providers that are readily available.

5 https://www.eff.org/deeplinks/2014/06/why-you-should-use-tor
3.3.4 Virtual Private Servers (VPS) / Bulletproof hosting

Actors may acquire a VPS to keep their attack tools and ill-gotten information away from their personal computers. This is yet another “cut-out” mechanism designed to distance the actor from the malicious activity and make the investigator’s job more difficult.

Malicious actors realize that any system on the Internet is susceptible to attack and so many professionals rely upon “bulletproof” hosting which cater to less than scrupulous actors and tout their ability to keep their customers safe. A VPS can employ VPN and anonymity network techniques to hide the nature and location of their VPS in the same way they can use the techniques to hide their entry point into the Internet.

3.3.5 Hop points / Compromised servers

Actors may infiltrate computer systems and networks which have no other use or interest to them than as separate hop between the actor’s computer and the actual target. Hop points may have no affiliation to the ultimate target, or actors can hop from trusted partner networks into their ultimate target.

Recently, Kaspersky Labs published a paper detailing the trade in compromised servers run out of the xDedic marketplace, one of many underground sites which offer access to compromised servers. The xDedic marketplace offered access to more than 70,000 servers. This is simply another form of VPS or hop point that the malicious actor can use as part of the tools in their OPSEC bag of tricks.

3.4 Cyber-criminal password quality

An interesting observation from the criminal forum database dumps are the passwords being used. HPE Security Research uses a password quality assessment system to recover passwords from cryptographic hashes. From this, the behaviors observed in password use and re-use provide interesting statistics. In some examples, having connected to real user accounts on legitimate sites with criminal actors, there is also password re-use. This means that some criminals use the same password on criminal controlled sites and on legitimate sites, like LinkedIn or Myspace – both of which had recent, high-profile password dumps.

The research included is using several criminal databases to generate reports and statistics on observed criminal password usage. We ran statistical programs on the recovered criminal password set as well as recovered set of passwords obtained from database dumps of legitimate websites in order to contrast and compare the two. The summary of observations follows.

The sheer size of the number of passwords from the legitimate database dumps required a random sampling of 10% to compare the password statistics against the set of criminal passwords recovered. In Figures 4 and 5 the top ten passwords for both cybercriminals (recovered hashes) and legitimate users (random sample) are revealed.

---

6 https://securelist.com/files/2016/06/xDedic_marketplace_ENG.pdf
There are many similarities between the two. The passwords 123456 and 123456789 are the top two passwords on both lists. The main difference is that 123456789 and 123456 appear less than one-tenth of one percent on legitimate sites while they appear 1.3% and 0.32% on the criminal sites. Following the trend across all of the top ten passwords reveals almost the same passwords with the frequency of use being far greater on the criminal side. This implies that criminals use common passwords more frequently which is more insecure and indicates bad OPSEC practices. The question is are criminals actually the worst offenders in terms of password quality?

Examining this further, figures 6 and 7 compare the top ten base words for both sample sets. This is where the difference starts to unfold as criminals use words like hacker, killer, master and expletives. On the legitimate list the top ten include love, mike, angel, and LinkedIn (this is due to the fact that a large number of passwords for this list came from the LinkedIn dump).

There are also many similarities between the two in usage of password and qwerty. Once again, the criminal side has a larger percentage of base word usage meaning criminals are more likely to use the same base words in making up their password but percentages are much lower so it is not as significant a problem as using the common passwords.

Next up is password length. This is an interesting peek into password complexity as it reveals the difficulty of password recovery if a brute force attack is attempted. Usually, when the user signs up for an account the site will suggest the password must be eight characters or longer.

In figures 8 and 9, 25% of the passwords from both lists are exactly eight characters long. Either users are most likely to use eight characters regardless of the minimum length required by sites or there are many sites that require a minimum of eight characters and users are simply wired to choose the shortest acceptable password length, which is more likely.
Looking into the password length a bit further, on the criminal side the next most common password is 6 characters long (20%) which leads us to believe that the most commonly required password length for criminal sites is six characters and is weaker in terms of security than required by many legitimate sites.

Figure 8  Top five most frequent password lengths for criminal sites.

Figure 9  Top five most frequent password lengths for legitimate sites.

This is not to say that password requirements for length is never six characters for non-criminal sites, but it is far less common as it represents less than 10% of passwords used.

The top five most common password lengths are six, seven, eight, nine and ten characters for both types. The only difference is in the actual usage, ten characters is the second most common password length for legitimate sites (23%) while for the criminal sites ten characters is the fourth most common (nearly 13%) a full 10% or more difference.

The next two figures (10 and 11) help explain password complexity in regards to length and character set usage. Almost 23% of all cracked criminal passwords are six characters or less in length while almost 40% are greater than eight characters. On the other hand, the legitimate site passwords contain less than 10% of passwords six characters or less and a little over 50% that are longer than 8 characters. This continues to support the belief that criminals use weaker passwords.

Figure 10  Distribution of password lengths and their character set complexity in criminal sites.

Figure 11  Distribution of password lengths and their character set complexity in legitimate sites.
25% of criminal passwords use lowercase alphabet characters (a-z) while only 13% of the legitimate passwords use the simple lowercase character set. The uppercase alphabet character set (A-Z) accounts for only around 0.3% for both criminal and legitimate password sets, which leaves numeric only.

Due to its small character set, numeric passwords are the easiest to recover, which shows a shockingly bad practice for legitimate users, but even more for users of criminal sites.

Almost 20% of the criminal passwords are numeric only, whereas legitimate passwords are less than 10% numeric only. Another check against criminal passwords for simple complexity.

Figures 12 and 13 provide more of a glimpse into the password complexity. There is a much greater frequency of lowercase alphanumeric passwords in legitimate than in criminal passwords.

What is not visible in these figure is that when it comes to legitimate passwords the users are choosing lowercase alphabet strings followed by 2-4 digits, generally representing a year. This pattern makes up the bulk of all legitimate passwords.

You can find the same pattern on the criminal side of things but at a much lower percentage, almost 30% less.

Another interesting take-away from the above figures is that criminal are less likely to use one or more special characters, which inherently makes their passwords less secure.

Looking into the use of special characters specifically in figures 14 and 15 below, almost the same five special characters are represented in both sets.

The top three are the same but in different frequency order of use. The glaring difference is once again the percentage of use.

Almost 5% of all legitimate passwords with special characters contained one of the top three special characters while only a little over 2% of the criminal passwords with special characters contained one of the top three special characters.
When combining the use of all the special characters the usage of top special characters in criminal passwords is around 5% while at the same time the usage of the top 5 special characters in legitimate passwords stands at around 10%. In other words, criminals are using special characters roughly half as much as legitimate users.

![Figure 14](image1.png)   ![Figure 15](image2.png)

**Figure 14** Top special characters used in criminal passwords.  **Figure 15** Top special characters used in legitimate passwords.

The last area examined is not related to password complexity, but rather the behavior and psychology of password usage.

The interesting thing to note is that the same two explicit words appear as the top two in both passwords sets although they differ in percentages. Users in criminal forums choose to include an explicit word in their password almost 2% of the time while users on legitimate sites are significantly less likely to use an expletive (0.7%). Criminal users are three times more likely to have an expletive or offensive slur in their password than a normal user.

Figure 16 shows the password recovery masks and the percentage of the passwords that match the mask for the criminal password set. The mask character ?d matches a number 0-9 while the mask character ?l matches a lowercase a-z. Not only are the masks interesting to analyze the passwords, but they can also be used by the advanced password recovery tool Hashcat to recover criminal passwords.

![Figure 16](image3.png)

**Figure 16** Top ten hashcat masks.
3.5 Malicious code OPSEC

There are number of techniques malicious actors tend to employ to minimize the chances of being flagged by the heuristic analysis of anti-virus (AV) engines, as well as avoid attribution from artifacts in the malware files created by them.

These methods help to avoid the creation of a unique imprint on the executable structure which would make it stand out from commonly available software. Some of these methods include:

- Use of common libraries and tools for system operations
- Avoiding the use of dedicated portable executable (PE) file protectors and custom made encryption routines as well as reuse of the encryption keys
- Avoiding the use of geographical references within a file or, better yet, use of random locale during the compilation time
- Avoiding the use of any name references within the file which can be traced to the origin of the file
- Use of tailored to custom operations and recompiled open source products
- Use of patched commercial DLLs
- Use of various levels of code optimizations during compilation time, striping the resulting file of debug information
- Use of malware kits which can be tailored and recompiled for a targeted operation

Generally, it is difficult to pin the use of a particular malware technique to a level of competency of a malicious actor or a group of actors. While it would be easy to think that the path of least resistance and quick availability of the results would be pertinent to malware actors with a low to medium skill level, advanced malicious groups often reuse readily available malware components while mounting an advance persistent threat attacks.

The uniqueness and complexity level of a particular malware technique may be used as an indicator of the skill level of a malware actor. For example, the Uroburos rootkit is a highly complex malware used to collect sensitive information. The complex design of the malware suggests the involvement of highly-skilled actors with a substantial financial backing. The features which makes this malware stand out include:

- Custom designed encrypted virtual file system
- Hooking a number of system calls to hide its activity
- Injecting proxy libraries between the user and the kernel space
- Using named pipes to virtualize network connections
- Modularity of the design allowing for a seamless upgrade

It is thought that the Uroburos malware was operational in the field for several years before being discovered. It is likely that there are a number of similarly designed rootkits by the same group of actors which are still going unnoticed while targeting high profile targets such as government institutions, research organizations and large private companies.

The level of malware complexity is not the only indicator of the attacker’s skill set. Another common indicator is the restricted nature of information used in order to make an attack successful. For example, the Automatic Teller Machine (ATM) malware GreenDispenser required industry insider knowledge of ATM operations as well as physical access to the internals of the actual ATM. These features indicate that it is most likely the creation of a well-organized group of skilled actors.

Another indication of actor sophistication is the exploitation of unpublished vulnerabilities (zero day). Discovery of these vulnerabilities and their subsequent exploitation require a high level of technical sophistication. Once a vulnerability is published and included in a tool set to be used by less advanced attackers it most likely reduces its usefulness to an advanced malware actor. Most of the time the AV industry is quick to catch up and devise countermeasures to published vulnerabilities rendering them useless for covert operations.
The following graph is useful in determining the sophistication of malware authors.

![Malware author sophistication graph](image)

**Figure 17** Malware author sophistication graph

### 3.6 OPSEC - Attribution and Advanced Persistent Threat (APT) actors

"On the Internet, nobody knows you’re a dog.” is the caption of the famous New Yorker cartoon which aptly captured what was at the time a new problem caused by the Internet, “how do we know who we are dealing with on the others side of the Internet?”

Though the cartoon was published in the July 5, 1993 issue, Peter Steiner, the cartoonist, put his finger jokingly upon what is still one of the more hotly debated subjects among information security professionals, that of attribution.

While knowing who is responsible for an attack is not technically required for incident responders to successfully remediate an intrusion, any experienced incident responder will tell you that knowing the team you are up against can help immensely. This is especially true when you know that a given actor is fond of using a specific technique or tool, and it hasn't yet detected that their intrusion has been discovered by the target’s security team.

The OPSEC methods discussed here should make obvious that all attackers, regardless of their motivation, have a myriad of tools and techniques at their disposal which help them hide. There is generally not much of a distinction between a competent, professional attacker and APT actors. Virtually all of the techniques used by other types of attacker are used by APT actors as well.
The question then becomes, “How can you pierce the OPSEC veil to better identify the actor that is responsible for an incident or campaign that you are engaged in?”

The key is to be found not so much in the fact that the actors use a VPN or TOR or hop points for their attacks. Rather, investigators look holistically at the pattern of an attack. This pattern includes, the goals of the actor, the industry or organization being targeted, TTPs (Tactics, Techniques and Procedures), and finally, the actual forensic or atomic evidence left behind, such as tools, IP addresses, domain registrations, and even the times when an actor is active.

This subject is addressed well in Mike Cloppert’s blog post titled “Security Intelligence: Attacking the Cyber Kill Chain” on the SANS Digital Forensics and Incident Response site.

Because of the sensitive nature of these patterns investigators are hesitant to share them, even in closed groups. The revelation of information used to identify an actor invariably causes the most cautious of actors to change part or all of the pattern in an attempt to regain a semblance of anonymity.

To use Steiner’s cartoon analogy, if you know someone can tell that you are a dog, you put a cat mask on. The empirical manifestation of this truth was born out when Mandiant released its seminal work on what they referred to as APT1. After Mandiant’s release of their findings, in the paper titled “APT1 Exposing One of China’s Cyber Espionage Units” Dan McWhorter wrote:

“Mandiant’s report and the simultaneous release of 3,000+ indicators hindered APT1’s operations by causing the group to retool and change some operational methodology. Since the report, APT1 has stopped using the vast majority of the infrastructure that was disclosed with the release of the indicators. However, APT1 maintained an extensive infrastructure of computer systems around the world, and it is highly likely that APT1 still maintains access to those systems or has utilized those systems to establish new attack infrastructure in the last three months.”

Another problem impeding proper attribution is one that also plagues the classification of malware samples. There is no standardized taxonomy used consistently across all organizations. A single actor can be referred to in public reports by a variety of names depending upon the research group writing the report. This is especially true of APT groups who do not need to sell their wares, or seek popularity among their peers. It is much less of a problem for groups which publicize their activities either in closed or public forums.

Correlating reports about the same actor when the name is not consistent makes it difficult to develop a complete corpus of all known instances of information regarding an actor that does not identify itself. One of the almost comical aspects of tracking APT actors is the emergence of “maps” that seek to aid in the cross-correlation of the myriad of names associated with a given actor.

---

9 https://www.fireeye.com/current-threats/threat-intelligence-reports.html?gclid=CNzZxtzthLUCFSbNOgogdGlwAsg
10 https://www.fireeye.com/blog/threat-research/2013/05/apt1-months-significantly-impacted-active-rebuilding.html
4 Conclusion

Operational security is a five stage process allowing practitioners to minimize the risk of their identities being exposed by their adversaries. Since one of the main goals of cybercriminals is to retain their cover, they must employ one or more OPSEC countermeasures described in this paper appropriate to their experience and skill level.

Our findings, however, show that cybercriminals frequently make OPSEC mistakes, and these mistakes represent a primary reason why their true identities are discovered by security researchers or law enforcement agents. In fact, our findings show that, on average, cybercriminal OPSEC is quite weak, which is best seen in the analysis of the strength of the password set recovered from the criminal underground forums database dumps in comparison with the strength of passwords recovered from legitimate database dumps resulting from breaches.

We believe that the OPSEC of cybercriminals, as well as other actors, will increase over time as the capability of security researchers and law enforcement agencies improve over time. Finally, we hope that this paper will be useful to security practitioners, law enforcement agencies and organizations trying to defend their infrastructure against cybercriminal attacks. By discovering what our adversaries know and how they approach their operational security we will be able to apply that knowledge to our own OPSEC process and better protect our own operations, resources and users targeted by cybercriminals and other adversarial actors.

List of figures

Figure 1 The OPSEC process....................................................................................................................................................................................... 2
Figure 2 Risk assessment matrix.............................................................................................................................................................................. 3
Figure 3 Top-rated VPN providers that are readily available..................................................................................................... 9
Figure 4 Top passwords used by cybercriminals...................................................................................................................................11
Figure 5 Top passwords used by users of legitimate sites...........................................................................................................11
Figure 6 Top ten base words used by cybercriminals......................................................................................................................11
Figure 7 Top ten base words used in legitimate passwords........................................................................................................11
Figure 8 Top five most frequent password lengths for criminal sites......................................................................................12
Figure 9 Top five most frequent password lengths for legitimate sites...........................................................................................12
Figure 10 Distribution of password lengths and their character set complexity in criminal sites........ 12
Figure 11 Distribution of password lengths and their character set complexity in legitimate sites........... 12
Figure 12 Top criminal password character sets...................................................................................................................................13
Figure 13 Top legitimate password character sets...................................................................................................................................13
Figure 14 Top special characters used in criminal passwords..............................................................................................................14
Figure 15 Top special characters used in legitimate passwords...........................................................................................................14
Figure 16 Top ten hashcat masks....................................................................................................................................................................... 14
Figure 17 Malware author sophistication graph...................................................................................................................................16

List of tables

Table 1 Ease of building block attribution based on the acquisition method of Building Blocks Based on Acquisition Method....................................................................................................................................................................................... 8
Authors and Contributors

This report is the result a collaboration of members of HPE Security Research.

Authors
Kevin Stevens
Bart Otten
Robin Jackson
Oleg Petrovsky
Vanja Svajcer

Contributors
Jewel Timpe