Designing Attack Infrastructure for Offensive Cyberspace Operations

Gazmend Huskaj[1, 2], Ion A. Iftimie[3, 4] and Richard L. Wilson[5,6]
[1]Swedish Defence University, Stockholm, Sweden
[2]University of Skövde, Skövde, Sweden
[3] Eisenhower PhD Fellow, NATO Defense College, Rome, Italy
[4] Senior Advisor, European Union Research Center, George Washington School of Business, Washington, D.C.
[5] Towson University, U.S.A.
[6] Senior Research Scholar, Hoffberger Center for Professional Ethics, University of Baltimore
gazmend.huskaj@fhs.se
iftimie@gwu.edu
wilson@towson.edu
DOI: 10.34190/EWS.20.077

Abstract: This article addresses the question 'what considerations should be taken by cyber commands when designing attack infrastructure for offensive operations?'. Nation-states are investing in equipping units tasked to conduct offensive cyberspace operations. Generating 'deny, degrade, disrupt, destroy or deceive' effects on adversary targets requires to move from own ('green'), through neutral ('grey'), to adversary ('red') cyberspace. The movement is supported by attack infrastructure for offensive cyberspace operations. In this paper, we review the professional and scientific literature identifying the requirements for designing an attack infrastructure. Next, we develop and define the concepts for attack infrastructure. Finally, we explain and describe the considerations for designing attack infrastructure. The research question is answered by proposing a framework for designing attack infrastructure. This framework is vital for military and civilian commands designing attack infrastructure for offensive cyberspace operations.

Keywords: Attack Infrastructure, Cyber Commands, Offensive Cyberspace Operations, Operational Security.

1. Introduction

Knowing how to design attack infrastructure supporting offensive operations is a relevant topic for cyber commands around the world. Nation-states are investing in civilian and military units to conduct offensive cyberspace operations. Generating 'deny, degrade, disrupt, destroy or deceive' effects on adversary targets requires to move from own ('green'), through neutral ('grey'), to adversary ('red') cyberspace. The movement is supported by attack infrastructure for offensive cyberspace operations. The case of WannaCry has demonstrated the impact uncontrolled weaponized code can have on civilian infrastructure (Chen and Bridges, 2017; Kao and Hsiao, 2018; Mohurle and Patil, 2017). The cases of Operation Cloud Hopper (Bird, 2015; Galinkin et al., n.d.; Vincent, 2019) and Operation Glowing Symphony (Iftimie, 2019; Jacobsen, 2019) have demonstrated the impact of controlled weaponized codes and required infrastructures to support these operations. Probing scientific databases reveals 15 articles on the topic. Probing red team literature also reveals numerous thoughts and ideas on attack infrastructure. Based on this review of literature, this study seeks to answer the following research question: what considerations should be taken by cyber commands when designing attack infrastructure for offensive operations?

The main contributions are summarized as follows:

1. attack infrastructure is described by conducting a review of the scientific and professional literature;
2. based on 1), concepts are developed and defined;
3. then, the considerations for designing attack infrastructure are explained and described;
4. finally, the design considerations for attack infrastructure are provided, followed by operational security and ethical considerations, and policy recommendations.

This study begins with a review of the professional and scientific literature identifying the requirements for designing an attack infrastructure. This results in a conceptual framework presented in Table 1. The research approach for this research is described in Section 3, and the attack infrastructure considerations are presented in Section 4. Section 5 develops theory for attack infrastructure. Sections 6 and 7 discuss Cybersecurity and

Ethical considerations, while Section 8 provides policy recommendations. Conclusions and future work are presented in Section 9.

2. The attack Infrastructure from practitioner and scientific points of view

Attack infrastructure is a requirement for conducting offensive cyberspace operations. Offensive cyberspace operations are defined as "a sequence of planned actions executed by an organized group of people with a defined purpose in and through hardware and software which are used to create, process, store, retrieve and disseminate information in different types of interconnected networks that build a large, global network, built and used by people" (Huskaj & Wilson, 2020). Offensive methods include, but are not limited to, obfuscation, redirection, and social engineering. The organized group of people requires infrastructure which enables the commands to reach the intended target(s). The design requirements for the attack infrastructure consist of segregation of duty, i.e. segregate Homebase or the forward operating base (FOB) from the C&C-server, phishing and payload servers.

The requirements for attack infrastructure consist of, domains, redirectors, servers for command & control (C2), phishing and payload delivery (Dimmock & Borosh, 2018). The domain should blend with the targets "baseline web traffic or fit with the social engineering campaign" (Dimmock, 2017). Redirectors are used to obfuscate and protect the Homebase or FOB from response actions. Two types of C2-servers exist: one for C2-actions on the target, and one to ensure permanence. The C2-server for permanence should never be used for actions on the target due to the risk of losing permanence (Mudge, 2014). They can also be used to redirect a target to the web site holding the payload (Dimmock, 2017). Social engineering and phishing attacks are used for payload delivery to the target (Dimmock & Borosh, 2018). Communication between the organized group, their C2-server to their other assets is always encrypted (Dimmock & Borosh, 2018; Feroze, 2018). These insights are supported by scientific research as depicted in Table 1.

Table 1: Summary of the required infrastructure, tools, techniques and procedures for offensive operations

Concept	Definition	Author
Abuse legitimate services	Creating malicious domain names	(Chiba D., Akiyama M., Yagi T., Yagi T., Mori T., Goto S., 2018)
Advanced Persistent Threat (APT)	Operate many domains and subdomains	(Liu D., Li Z., Du K., Wang H., Liu B., Duan H., 2017)
Backdoors	Malware that opens ports and calls the C&C, enabling an attacker to take actions in the target system	(Hrad O., Kemppainen S., 2016; Leontiadis N., Moore T., Christin N., 2014)
Brute-forcing	To gain access into a system	(Hrad O., Kemppainen S., 2016; Liu D., Li Z., Du K., Wang H., Liu B., Duan H., 2017)
Buffer overflow	Enables putting more data in memory causing execution of code	(Mimura M., Tanaka H., 2017)
C&C	Send commands to the target	(Chiba D., Akiyama M., Yagi T., Yagi T., Mori T., Goto S., 2018; Hrad O., Kemppainen S., 2016)
Collection and threat collection	Collecting information about the target system, but also exfiltrating information once inside the target	(Antonatos S., Akritidis P., Lam V.T., Anagnostakis K.G., 2008; Alrwais S.A., Dunn C.W., Gupta M., Gerber A., Spatscheck O., Osterweil E., 2012; Kim N., Lee S., Cho H., Kim B.-I., Jun M., 2018)
Content delivery network (CDN)	Use them to deliver malware	(Chiba D., Akiyama M., Yagi T., Yagi T., Mori T., Goto S., 2018)
Cyber sanctions	The actual or threatened restriction of digital transactions to affect a behavioral change by the target through the introduction of psychological pressure against its political leaders and populace	(Iftimie I., 2019)
DDoS - NTP, TCP	Various protocols may be used to conduct DDoS-attacks	(Berti-Equille L., Zhauniarovich Y., 2017; Collier B., Thomas D.R., Clayton R., Hutchings A., 2019; Karami M., Park Y., McCoy D., 2016; Krupp J., Backes M., Rossow C., 2016; Mezzour G., Carley K.M., Carley L.R., 2017)
Directory traversal	Enables access to restricted directories in a web-server	(Mimura M., Tanaka H., 2017)

Concept	Definition	Author
DNS misconfiguration, reliable, malicious resolver	DNS are reliable infrastructure to use for beacon-sending and C&C	(Alrwais S.A., Dunn C.W., Gupta M., Gerber A., Spatscheck O., Osterweil E., 2012; Chiba D., Akiyama M., Yagi T., Yagi T., Mori T., Goto S., 2018; Karami M., Park Y., McCoy D., 2016)
Domains	Using domains, domain-names, sub-domains and domain generation algorithms to create new infrastructure and increase success rate of attacks which can resemble well-known legitimate domains	(Chiba D., Akiyama M., Yagi T., Yagi T., Mori T., Goto S., 2018; Kim N., Lee S., Cho H., Kim B.-I., Jun M., 2018; Liu D., Li Z., Du K., Wang H., Liu B., Duan H., 2017; Lu L., Perdisci R., Lee W., 2011)
Example infrastructure	Brute force into a target, pass info to C&C, which then downloads additional software	(Hrad O., Kemppainen S., 2016; Mezzour G., Carley K.M., Carley L.R., 2017)
Exploits, Kit, Angler, Blackhole Toolkit	Tools to conduct actions on the target	(Leontiadis N., Moore T., Christin N., 2014; Liu D., Li Z., Du K., Wang H., Liu B., Duan H., 2017; Mezzour G., Carley K.M., Carley L.R., 2017)
Fake applications	Deceiving the user to install it, and once installed, asks user to pay premium, or ransomware	(Mezzour G., Carley K.M., Carley L.R., 2017)
HTTP	A protocol to distribute exploits or malware and for C&C	(Chiba D., Akiyama M., Yagi T., Yagi T., Mori T., Goto S., 2018; Mimura M., Tanaka H., 2017)
Information systems - malicious that launch attacks	Own systems or hijacked systems used for further attacks	(Mezzour G., Carley K.M., Carley L.R., 2017)
Injection	Injecting scripts into parent web-documents	(Alrwais S.A., Dunn C.W., Gupta M., Gerber A., Spatscheck O., Osterweil E., 2012)
IP addresses, and malicious	Many IP-addresses are required to conduct operations because some may be burned while conducting operations	(Alrwais S.A., Dunn C.W., Gupta M., Gerber A., Spatscheck O., Osterweil E., 2012; Lu L., Perdisci R., Lee W., 2011; Kim N., Lee S., Cho H., Kim B.-I., Jun M., 2018)
Internet Service Providers (ISPs)	Get IP-addresses from many different ISPs to conduct attacks and for resilience	(Alrwais S.A., Dunn C.W., Gupta M., Gerber A., Spatscheck O., Osterweil E., 2012)
Malware, ransomware, trojan	Software to achieve effects. Malicious from the victim's perspective	(Hrad O., Kemppainen S., 2016; Kim N., Lee S., Cho H., Kim B.-I., Jun M., 2018; Leontiadis N., Moore T., Christin N., 2014; Liu D., Li Z., Du K., Wang H., Liu B., Duan H., 2017)
MitM	Man-in-the-middle attack to extract credentials used for future attacks	(Almeshekah M.H., Atallah M.J., Spafford E.H., 2015)
Obfuscation	Making it difficult for the target/defenders to identify the attackers motives	(Antonatos S., Akritidis P., Lam V.T., Anagnostakis K.G., 2008)
Persistence	Have presence on many different targets that enable access if some targets are identified and blocked by the defenders	(Leontiadis N., Moore T., Christin N., 2014; Lu L., Perdisci R., Lee W., 2011)
Phishing - Harvesting credentials	Deceiving the user to download and run a file, or click on a link which enables access to a target	(Almeshekah M.H., Atallah M.J., Spafford E.H., 2015; Alrwais S.A., Dunn C.W., Gupta M., Gerber A., Spatscheck O., Osterweil E., 2012; Liu D., Li Z., Du K., Wang H., Liu B., Duan H., 2017)
Privilege escalation	Using the privileges of newly gained access in a target for future actions	(Hrad O., Kemppainen S., 2016)
Re-registration	Re-registering domain names to increase chance of success of attacks	(Chiba D., Akiyama M., Yagi T., Yagi T., Mori T., Goto S., 2018)
Redirection - and click link	Use various techniques to redirect users to website that enables attack success	(Alrwais S.A., Dunn C.W., Gupta M., Gerber A., Spatscheck O., Osterweil E., 2012; Leontiadis N., Moore T., Christin N., 2014; Liu D., Li Z., Du K., Wang H., Liu B., Duan H., 2017; Lu L., Perdisci R., Lee W., 2011; Mezzour G., Carley K.M., Carley L.R., 2017)
Reflection attack	Using various protocols to conduct amplify attack traffic	(Karami M., Park Y., McCoy D., 2016)
Rootkits	Software hidden from the target, enables persistence	(Hrad O., Kemppainen S., 2016)

Concept	Definition	Author
Search poison - engine poisoning	Use popular keywords to cause user interaction which then are redirected to the attackers site	(Leontiadis N., Moore T., Christin N., 2014; Lu L., Perdisci R., Lee W., 2011)
Sinkholing	Redirecting network traffic from the intended destination to the attackers information system	(Chiba D., Akiyama M., Yagi T., Yagi T., Mori T., Goto S., 2018)
Social engineering	Various techniques to deceive the user into various actions; download file, click on link, give credentials	(Liu D., Li Z., Du K., Wang H., Liu B., Duan H., 2017)
Spoofing	Spoofing the target's source address overwhelming them with network traffic denying access to services	(Karami M., Park Y., McCoy D., 2016)
Triggering	Strings that trigger browser-specific code, such as redirection	(Antonatos S., Akritidis P., Lam V.T., Anagnostakis K.G., 2008; Leontiadis N., Moore T., Christin N., 2014)
Web exploitation	Techniques that enable access to a target. Web architecture-compromising server, HTML, Javascript, browser, hosting sites for phishing, exploit browser to deliver malware via advertising ecosystem, cross-site scripting, man-in-the-browser, malicious iFrames, Drive-by-download	(Almeshekah M.H., Atallah M.J., Spafford E.H., 2015; Alrwais S.A., Dunn C.W., Gupta M., Gerber A., Spatscheck O., Osterweil E., 2012; Antonatos S., Akritidis P., Lam V.T., Anagnostakis K.G., 2008; Chiba D., Akiyama M., Yagi T., Yagi T., Mori T., Goto S., 2018; Liu D., Li Z., Du K., Wang H., Liu B., Duan H., 2017; Mezzour G., Carley K.M., Carley L.R., 2017; Mimura M., Tanaka H., 2017)

3. Research approach

Academic research on attack infrastructure for offensive operations is limited. The identified research is primarily focused on defensive measures by first noting attacker-tools, tactics, techniques and procedures (herein modus). Then, after the threat's modus is described, the researchers discuss various defensive measures. The search for academic articles, used the string "attack infrastructure." It was done in Elsevier's Scopus® database, the ACM Digital Library, and IEEE Xplore®, resulting in 14, 22, and 8 document results respectively. Next, all of the documents were manually reviewed by GH. The requirements for an article to be within scope for inclusion were: it must discuss attack infrastructure, methods, tools, tactics, techniques and procedures. The exclusion criteria were articles beyond scope and doubles. Therefore, the final articles for review amounted to 15, which are also depicted in Table 1.

The same criteria applied when searching for professional documents on the topic. However, the search string used in a search engine (Google), was "red team attack infrastructure" without the apostrophes. The listed results were manually reviewed by GH, and snowballing began with Leibowitz & Timzen (2019). The included professional sites are: Kohlenberg (2018); Feroze (2018); Gimmick & Borosh (2018); Dimmock (2017); and Mudge (2014).

The results of the collected data were twofold: the research dataset is already mentioned above, while the "professional" dataset discussed design requirements on attack infrastructure, operational security, and behavior of red team operators when conducting offensive operations. These two perspectives are noted in section 2.

4. Components in Attack Infrastructure

The domain name system (DNS) is a critical part of attack infrastructure. It is a critical function of the Internet: it maps the IP-address of an information system to a name. Information systems are better at managing numbers while humans are better at managing names. For example, the IP-address `127.0.0.1`, "assigned for use as the Internet host `loopback` address" (Cotton & Vega, 2010), is also known as "`localhost`", i.e. this computer (Cheshire & Krochmal).

DNS is a distributed system of databases and "is based on a hierarchical database containing resource records (RRs) that include the name, IP address, and other information about hosts" (Stallings, 2006, p.777). The RRs are many, but those of primarily importance are the A and NS records. The A record maps the IP address to a the system name, e.g.: `127.0.0.1 localhost`. The NS record points to the authoritative name server for this particular domain (Stallings, 2006). `example[.]com` is an example domain with the NS-record `ns1.example[.]com`. The A record is used to point domains to redirectors (more on redirectors below) and team servers (Mudge, 2014).

Therefore, using domains, domain-names, sub-domains to create new infrastructure that resembles well-known legitimate domains increases the success rate of attacks. In the 'Operation Cloud Hopper' case, attackers used domains such as `mailserever[.]com`, `mailsserver[.]com`, and `mailvserver[.]com` (PwC, 2017). These are domain names where a user may be tricked into believing are legitimate mail servers, but in fact are not. The second way to generate domains quickly are domain generation algorithms (DGA). A DGA is implemented in the weaponized code to constantly provide it with new domains on the fly for communications to the command and control server (Arntz, 2016; Scarfo, 2016). Examples include `uqhucsontf[.]com`, `myypqmvzkgnrf[.]com`, `ocufxskoiegqvv[.]com` (Scarfo, 2016). In the 'Operation Cloud Hopper' case, 1375 domain names were used in that operation (PwC & BAE Systems, 2017). This shows that it is recommended to have multiple domain names for operations.

4.1 Command and control servers (C2)

C2 servers ensure that communication flows between Homebase and the target. The complexity of the Internet, various protocols and services, makes it possible to utilize the same for C2. The first step however, is to establish a front domain. The front domain serves the purpose of being a legitimate channel enabling communications to/from the target, and to/from the C2-server. Using a legitimate domain makes it easier to blend in with other communications in the target's infrastructure and reduces the likelihood of being spotted. Examples of legitimate domains are DropBox, and OneDrive (Sharma & Singh, 2018), or Google hosts, e.g. `google[.]com`, `gmail[.]com`, `mail.google[.]com` (Nahari, 2017). The target-type decides which front domain is used based on the collection phase on the target.

4.2 Redirectors

Redirectors are servers that, as the name implies, redirect communications from/to the target to/from the Homebase. Two versions exist: one for ongoing operations (known as short haul) and one for maintaining presence in the target (long haul). The Homebase can have one or several redirectors in front for operation security, by making it more difficult for the adversary to find Homebase and related infrastructure. The short haul servers are used to take actions on the target (Mudge, 2014; Sharma & Singh, 2018). The short haul servers are protected by one or more redirectors, and if a defender takes action, only the identified short haul server is destroyed. This enables conducting actions on the target through another redirector while simultaneously deploying a new redirector to take the place of the previously destroyed one. The long haul servers are used to ensure permanence in the target (Mudge, 2014; Sharma & Singh, 2018). The difference with the short haul servers is that long haul servers have longer callback timers to C2 indicating they're alive. The pre-determined time (days, weeks, months, years) of the offensive operation determines the callback timer, which could be once every 24 hours, to more (Mudge, 2014).

4.3 Phishing and payload delivery

Deceiving the user to download and run a file, or click on a link which delivers the payload and enables access to a target's information system is the purpose of phishing. Collection on the target decides which type of payload(s) should be chosen: "HTML Applications (HTAs), Embedded OLE objects in Office documents, Office macros, and Windows shortcut (LNK) files" (Dimmock, 2017). Two possible courses of action (COAs) exist: 1) based on collection, choose one or several of the payload types and deploy them from own owned servers, cloud providers, or hijacked servers; 2) based on collection, create a test-bed environment, conduct tests on that, and based on the results, adjust payload and payload delivery. Just as with other infrastructure, one or several redirectors should be put in front of the payload delivery server to protect it from defenders.

4.4 Encryption

Encryption should be a standard feature to ensure communications are not eavesdropped by a third party. OpenSSL with a custom generated certificate, or a legitimate one, or by impersonating another vendor, can be used to encrypt communications to/from the target (Sharma & Singh, 2018). Encryption is also needed to make it difficult for defenders to detect payloads by using payloads that offer encryption (Sharma & Singh, 2018).

4.5 Protection

C2 servers, stagers and payload deliverers are high-value infrastructure. Protecting them by deploying redirectors in front of them has already been mentioned. Additional actions to be taken include enabling firewall rules on these assets. The firewall rules should only allow the infrastructure under the organized group's control the ability to connect to C2, stagers, redirectors and payload deliverers (Sharma & Singh, 2018).

5. Design Considerations: Framework Development

America's International Technology Education Association defines design "as an iterative decision-making process that produces plans by which resources are converted into products or systems that meet human needs and wants or solve problems" (Banach and Ryan, 2009, p. 105). Within the context of an attack infrastructure for offensive cyberspace operations, design is a conceptual stage, which precedes the more concrete planning and building/execution stages of the attack infrastructure. Figure 1 gives an overview of the design considerations for attack infrastructure supporting offensive operations. This is supported by scientific literature and professional literature. The policy level tasking the organized group to conduct operations is not considered. It is assumed that the policy level have given the green light/"GO" to conduct offensive operations.

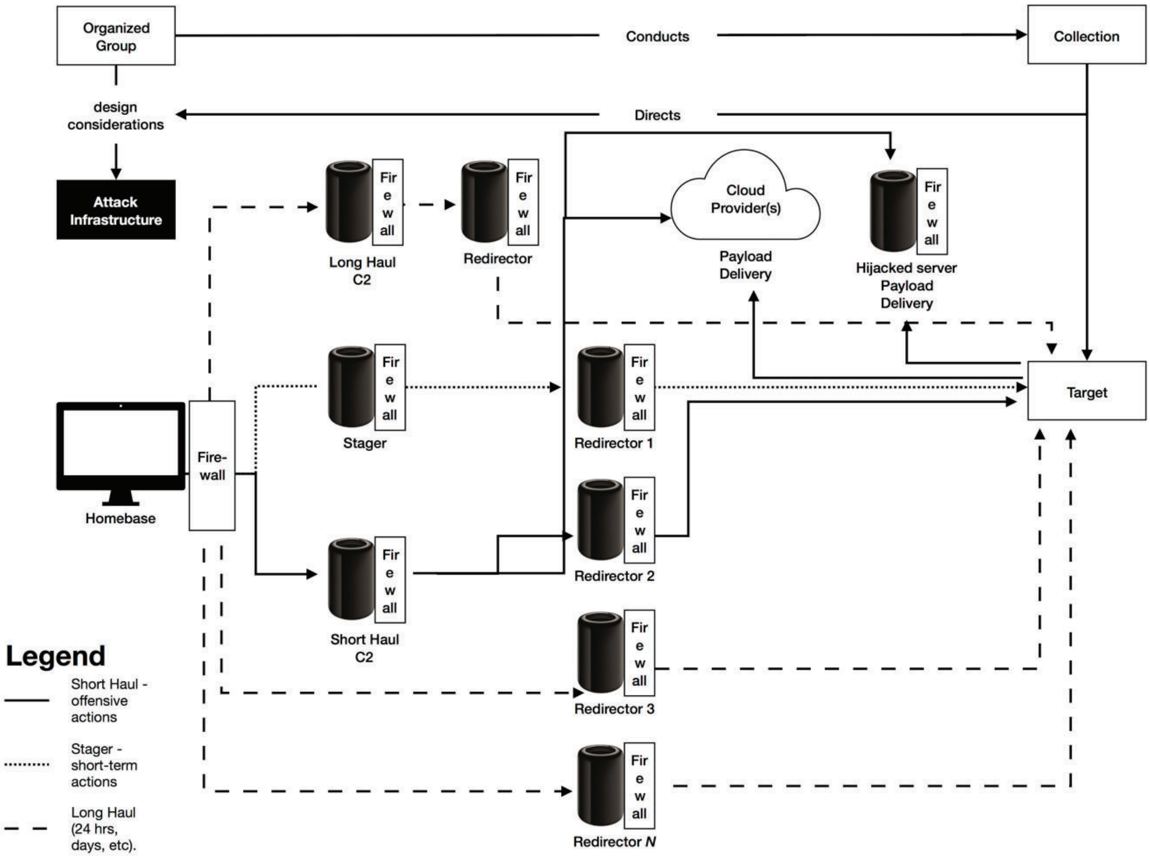

Figure 1: Simplified example of design considerations for attack infrastructure

The organized group begins by conducting intelligence collection on the target organization. Collection can target numerous open sources like social media, the organization's website(s), and `whois`. Collection also determines what kind of operating system(s), web pages, services (e.g. OneDrive, DropBox, etc.), sensors (e.g. intrusion detection systems and anti-virus systems) the target is using. Many tools exist that can automate this stage. This information results in a list of assets which directs collection to vulnerability databases and exploit databases, directing offensive methods. Furthermore, applying machine learning algorithms on employees in the target organization enables generating near-perfect profiles. These profiles may then be used to generate spear-phishing e-mails, with attachments or links. The attachments or links will then redirect the target user to one or several payload sites. These sites are either hosted on cloud provider's infrastructure, or in hijacked servers. One key requirement is encrypting the payload to avoid detection by various sensors in the target, such as intrusion detection systems and anti-virus systems.

Designing the infrastructure requires many domain names, either close to impersonation of legitimate ones, or hiding behind legitimate ones. To register domain names, scripts can be used to generate human readable domains like `mailserever[.]com`, `mailsserver[.]com`, and `mailvserver[.]com`. Another option is to employ a DGA to generate domains like `uqhucsontf[.]com`, `myypqmvzkgnrf[.]com`, and `ocufxskoiegqvv[.]com`. The servers which the domain names point to are used as redirectors, long haul C2, short haul C2, and for staging attacks. Each of these high-value assets have a redirector in front of them with a firewall. The purpose is to make it harder for defenders to trace the operation. Finally, once the payload is delivered to the target, and activated, the stager is used to establish permanence by adding additional software which calls back to the long haul C2 every 24 hours or more; and software which calls back to the short haul C2. The operators will then use the short haul C2-server to conduct further actions. These actions can be to conduct more collection to learn the infrastructure, position additional software for long haul C2, but also create escalate privileges of existing users to avoid detection by creating new users.

6. Operational Security Considerations

Similarly to the concept of protection, which uses firewalls to conceal attack infrastructure, the primary operational security considerations are those of using hardware and software that insures security of the attack infrastructure as well as tactics, techniques, and procedures (TTPs) that conceal the attack infrastructure's design, functions, and attribution of users.

First, software and hardware used in the attack infrastructure must be secure. This means that when considering updates to the software and hardware of the attack infrastructure, a serious discussion should take place whether to implement the updates or not and weigh the risks about potential effects on the infrastructure, and ongoing offensive operations.

Secondly, the issue of attribution of attack infrastructure must be addressed. If any node (hardware or software) or TTP of the attack infrastructure can be attributed to it, this endangers not only the attack infrastructure, but also the success of offensive cyberspace operations and the safety of the military and/or civilian units conducting them. For this reason, operational security is of outmost significance for the design of attack infrastructure for offensive cyberspace operations. Lack of operational security during the design of attack infrastructure for offensive cyberspace operations has led in the past not only to attribution of attack infrastructures, but also to the identities of their users. For example, attribution of many Chinese and Russian intelligence officers that ended up on the FBI Cyber's Most Wanted list was made possible by failed Chinese and Russian designs of attack infrastructure for cyberspace operations.

7. Ethical Considerations

The primary ethical issues here are using cloud service provider's infrastructure for payload deliver, hijacking servers to do the same, and impersonating legitimate actors. Furrow (2005) states that ethics is related to evaluating actions done by those who are capable of being moral agents. The focus can be on the person, intent, motive the act or the impact. The ethical issues are identified by asking four questions: 1) what actions are performed when taking actions to deploy a payload and/or impersonate a legitimate actor; 2) what is the character of the person(s) conducting those actions; 3) what are their intentions; and 4) what are the consequences of the payloads. These questions can be analyzed by applying a set of rules developed by a community of scholars. A set of 5 rules have been developed by a community of scholars to help guide thoughts about computing artifacts which in this case are taken to be the result of the development of attack infrastructure. (Miller, Keith, Moral Responsibility for Computing Artifacts: Five Rules, Version 24). These 5 rules were developed to help guide how technological artifacts should be designed and used. In this analysis attack infrastructure for offensive cyberspace operations are taken to fall into this category. In order to apply the 5 rules we assume that attack infrastructure for offensive cyberspace operations, and associated technologies and artifacts, are all sophisticated technological artifacts.

The first rule states, "The people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact. This responsibility is shared with other people who design, develop, deploy or knowingly use the artifact as part of a sociotechnical system." The application of this rule would be that the creators of the applications of the technologies related to attack infrastructure for offensive cyberspace operations need to be aware of the impact of their operations on users and that users should be aware of the impact of attack infrastructure technology and they are responsible for employing attack infrastructure technology in a socially responsible way.

The second rule of the 5 states, “The shared responsibility of computing artifacts is not a zero-sum game. The responsibility of an individual is not reduced simply because more people become involved in designing, developing, deploying or using the artifact. Instead, a person’s responsibility includes being answerable for the behaviors of the artifact and for the artifact’s effects after deployment, to the degree to which these effects are reasonably foreseeable by that person.” This second rule would state that those engaged in the development of artifacts employing attack infrastructure for offensive cyberspace operations should be responsible for the creation of this infrastructure and for what the application of this technology can accomplish, as well as for the social impact of the attack infrastructure employed for offensive cyberspace operations.

The fifth rule of the 5 rules is, “People who design, develop, deploy, promote, or evaluate a computing artifact ‘such as attack infrastructure for offensive cyberspace operations’ should not explicitly or implicitly deceive users about the artifact or its foreseeable effects, or about the sociotechnical systems in which the artifact is embedded.” One application of this rule would be that the designers of attack infrastructure should make it transparent to users and to members of society how applications have a social impact. It needs to be made clear to stakeholders how attack infrastructure is being used, and designers should provide a simplistic way for users to understand how the technology works. The purpose is to guide thoughts on attack infrastructure for offensive cyberspace operations and how these activities affect sociotechnical systems attacked by offensive cyber operations.

The conclusions that can be drawn from this ethical analysis are that 1) the organized group conducting offensive operations are doing so under the orders given by the policy level in a nation state. Rule-based nation states adhere to International law and the law of armed conflict. Next, 2) the character of personnel conducting those actions fit within a nation state’s predetermined set of criteria, excluding those who do not fit. Then 3), the intentions are those of the nation state. Finally, 4) the consequences of the payloads are those which have gone through a thorough internal national review. The biggest challenge is rule five, and deception. However, as mentioned above, the nation state directs the developer, and if this conflicts with the developer’s own moral compass, the developer is replaced.

8. Policy Recommendations

The conclusions of the ethical considerations form the basis of anticipatory ethical considerations/policy. It is anticipated that designing attack infrastructure for offensive operations require major collection efforts on human targets, on the target’s information systems, and infrastructure. Next, the organized group should demonstrate to policy makers how infrastructure is designed to increase their knowledge so they get more comfortable on this supports offensive operations.

9. Conclusions

The answer to the research question of ‘what design considerations should be taken when designing attack infrastructure for offensive operations?’ is noted in the framework development section. The ethical considerations are that developers and designers are morally responsible for the computer artefacts they generate, and their consequences. However, rule-based nation states adhere to international law and the law of armed conflicts. Therefore, people in the organized group that are designing attack infrastructure and developing payloads have legal support and policy support. The challenge is nation states who do not adhere to international law, the law of armed conflict, and employ proxies like cyber criminals, or patriotic hackers. Future research could include to develop an attack infrastructure in a virtual environment separated from the Internet. The environment can be used to train operators in the organized group, but also develop tools, tactics, techniques and procedures.

References

Alrwais, S. A., Dunn, C. W., Gupta, M., Gerber, A., Spatscheck, O., & Osterweil, E. (2012). Dissecting Ghost Clicks: Ad fraud via misdirected human clicks. ACM International Conference Proceeding Series, 21–30. https://doi.org/10.1145/2420950.2420954.

Antonatos, S., Akritidis, P., Lam, V. T., & Anagnostakis, K. G. (2008). Puppetnets: Misusing web browsers as a distributed attack infrastructure. ACM Transactions on Information and System Security, 12(2), 1–38. https://doi.org/10.1145/1455518.1455524.

Arntz, P. (2016). Explained: Domain Generating Algorithm. Retrieved from https://blog.malwarebytes.com/security-world/2016/12/explained-domain-generating-algorithm/.

Banach SJ and Ryan A (2009) The art of design: A design methodology. apps.dtic.mil. Available at: https://apps.dtic.mil/docs/citations/ADA518192.

Berti-Equille, L., & Zhauniarovich, Y. (2017). Profiling DRDoS attacks with data analytics pipeline. International Conference on Information and Knowledge Management, Proceedings, Part F1318, 1983–1986. https://doi.org/10.1145/3132847.3133155.

Bird J (2015) NATO's Role in Counter-Terrorism. *Perspectives on Terrorism* 9(2). Available at: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/419/html (accessed 1 September 2019).

Chen Q and Bridges RA (2017) Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware. In: *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, December 2017, pp. 454–460. ieeexplore.ieee.org.

Cheshire, S., Krochmal, M. (2013). Special-Use Domain Names. Retrieved from https://tools.ietf.org/html/rfc6761.

Chiba, D., Akiyama, M., Yagi, T., Hato, K., Mori, T., & Goto, S. (2018). DomainChroma: Building actionable threat intelligence from malicious domain names. Computers and Security, 77, 138–161. https://doi.org/10.1016/j.cose.2018.03.013.

Collier, B., Clayton, R., Thomas, D. R., & Hutchings, A. (2019). Booting the booters: Evaluating the effects of police interventions in the market for denial-of-service attacks. Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC, 50–64. https://doi.org/10.1145/3355369.3355592.

Connolly, L., Lang, M., & Tygar, J. D. (2015). ICT Systems Security and Privacy Protection. IFIP Advances in Information and Communication Technology, 455, 283–296. https://doi.org/10.1007/978-3-319-18467-8.

Cotton, M., Vegoda, L. (2010). Special Use IPv4 Addresses. Retrieved from https://tools.ietf.org/html/rfc5735.

Dimmock, J. (2017). Designing Effective Covert Red Team Attack Infrastructure. Retrieved from https://bluescreenofjeff.com/2017-12-05-designing-effective-covert-red-team-attack-infrastructure/.

Dimmock, J., & Borosh, S. (2018). Red Team Infrastructure Wiki. Retrieved from https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki.

Feroze, R. (2018). RedTeaming from Zero To One – Part 1. Retrieved from https://payatu.com/redteaming-from-zero-to-one-part-1.

Furrow, D. (2005). Ethics (Key Concepts in Philosophy). Bloomsbury.

Galinkin E, Jenko Hwong AS, Estep C, et al. (n.d.) The Future of Cyber Attacks and Defense is in the Cloud. Available at: https://www.researchgate.net/profile/Raymond_Canzanese/publication/336592029_The_Future_of_Cyber_Attacks_and_Defense_is_in_the_Cloud/links/5da78744299bf1c1e4c82fb0/The-Future-of-Cyber-Attacks-and-Defense-is-in-the-Cloud.pdf (accessed 27 January 2020).

Hrad, O., & Kemppainen, S. (2016). Honeypot utilization for analyzing cyber attacks. In Proceedings of the 10th European Conference on Software Architecture Workshops - ECSAW '16 (Vol. 222, pp. 1–2). New York, New York, USA: ACM Press. https://doi.org/10.1145/2993412.2993415.

Huskaj, G., Wilson, R.L., (2020). An Anticipatory Ethical Analysis of Offensive Cyberspace Operations. Proceedings of 15th International Conference on Cyber Warfare and Security (ICCWS), Norfolk, Virginia, U.S.A.

Iftimie IA (2019) Cyber Sanctions: The Embargo of Flagged Data in a Geo-Cultural Internet. In: *18th European Conference on Cyber Warfare and Security*, Reading, UK, 2019. Academic Conferences and Publishing International Limited.

Jacobsen JT (2019) NATOs offensive cyberspaceoperationer. Muligheder og udfordringer ved NATOs forespørgselsdrevne og effektbaserede tilgang. *Internasjonal Politikk* 77(3). tidsskriftet-ip.no: 241–251.

Kao D and Hsiao S (2018) The dynamic analysis of WannaCry ransomware. In: *2018 20th International Conference on Advanced Communication Technology (ICACT)*, February 2018, pp. 159–166. ieeexplore.ieee.org.

Karami, M., Park, Y., & McCoy, D. (2016). Stress testing the booters: Understanding and undermining the business of DDoS services. 25th International World Wide Web Conference, WWW 2016, 1033–1043. https://doi.org/10.1145/2872427.2883004.

Kim, N., Lee, S., Cho, H., Kim, B. I., & Jun, M. S. (2018). Design of a Cyber Threat Information Collection System for Cyber Attack Correlation. 2018 International Conference on Platform Technology and Service, PlatCon 2018, (2016), 1–6. https://doi.org/10.1109/PlatCon.2018.8472775.

Kohlenberg, T. (2018). Red Teaming. A Conference for Defence. Retrieved from https://www.youtube.com/watch?v=P4zIUQQo6Hg.

Krupp, J., Backes, M., & Rossow, C. (2016). Identifying the scan and attack infrastructures behind amplification DDoS attacks. Proceedings of the ACM Conference on Computer and Communications Security, 24-28-Octo(i), 1426–1437. https://doi.org/10.1145/2976749.2978293.

Leibowitz, M., & Timzen, T., (2019). Attack Infrastructure for the Modern Red Team. Retrieved from https://speakerdeck.com/tophertimzen/attack-infrastructure-for-the-modern-red-team.

Leontiadis, N., Moore, T., & Christin, N. (2014). A Nearly Four-Year Longitudinal Study of Search-Engine Poisoning Categories and Subject Descriptors. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 930–941. https://doi.org/10.1145/2660267.2660332.

Liu, D., Li, Z., Du, K., Wang, H., Liu, B., & Duan, H. (2017). Don't Let One Rotten Apple Spoil the Whole Barrel. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17 (pp. 537–552). New York, New York, USA: ACM Press. https://doi.org/10.1145/3133956.3134049.

Lu, L., & Lee, W. (2011). SURF : Detecting and Measuring Search Poisoning Categories and Subject Descriptors. Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS '11), 467–476. https://doi.org/10.1145/2046707.2046762.

Mezzour, G., Carley, K. M., & Carley, L. R. (2017). Global variation in attack encounters and hosting. ACM International Conference Proceeding Series, Part F1271, 62–73. https://doi.org/10.1145/3055305.3055306.

Miller, K., Moral Responsibility for Computing Artifacts: Five Rules, Version 24, IT Professional, 13(3):57 – 59, July 2011.

Mimura, M., & Tanaka, H. (2018). Long-Term Performance of a Generic Intrusion Detection Method Using Doc2vec. Proceedings - 2017 5th International Symposium on Computing and Networking, CANDAR 2017, 2018-Janua, 456–462. https://doi.org/10.1109/CANDAR.2017.

Mohurle S and Patil M (2017) A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science* 8(5). International Journal of Advanced Research in Computer Science. Available at: https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf.

Mudge, R. (2014). Infrastructure for Ongoing Red Team Operations. Retrieved from https://blog.cobaltstrike.com/2014/09/09/infrastructure-for-ongoing-red-team-operations/.

Nahari, S. (2017). Red Team Insights on HTTPS Domain Fronting Google Hosts Using Cobalt Strike. Retrieved from https://www.cyberark.com/threat-research-blog/red-team-insights-https-domain-fronting-google-hosts-using-cobalt-strike/.

PwC., BAE Systems., (2017). Operation Cloud Hopper - Indicators of Compromise. Retrieved from https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-indicators-of-compromise-v3.pdf.

Scarfo, A. (2016). Domain Generation Algorithms - Why so effective?. Retrieved from https://umbrella.cisco.com/blog/2016/10/10/domain-generation-algorithms-effective/.

Sharma, H., & Singh, H. (2018). Hands-on red team tactics. Birmingham: Packt Publishing Ltd.

Stallings, W. (2006). Data and computer communications (8th ed.). Pearson Prentice Hall.

Vincent A (2019) Don't feed the phish: how to avoid phishing attacks. *Network Security* 2019(2). Elsevier: 11–14.