2018 10th International Conference on Cyber Conflict
CyCon X: Maximising Effects
T. Minárik, R. Jakschis, L. Lindström (Eds.)
2018 © NATO CCD COE Publications, Tallinn

Aladdin's Lamp: The Theft and Re-weaponization of Malicious Code

Kārlis Podiņš
CERT Latvia
Riga, Latvia

Kenneth Geers
Comodo Group
Toronto, Canada

Abstract: Global superpowers do not have a monopoly on cyber warfare. Software thieves can steal malware written by more advanced coders and hackers, modify it, and reuse it for their own purposes. Smaller nations and even non-state actors can bypass the most technically challenging aspects of a computer network operation – vulnerability discovery and exploit development – to quickly acquire world-class cyber weapons. This paper is in two parts. First, it describes the technical aspects of malware re-weaponization, specifically the replacement of an existing payload and/or command-and-control (C2) architecture. Second, it explores the implications of this phenomenon and its ramifications for a range of strategic concerns including weapons proliferation, attack attribution, the fog of war, false flag operations, international diplomacy, and strategic miscalculation. And as with Aladdin's magic lamp, many malware thieves discover that obtaining a powerful new weapon carries with it risks as well as rewards.

Keywords: *malware, cyberwar, re-weaponization, false flag, attribution*

1. INTRODUCTION: STEALING CYBER WEAPONS

In *Arabian Nights*, a poor but clever Aladdin finds a magic lamp offering power, wealth, and love. However, the acquisition of these benefits also carried a burden of risk and responsibility. This parable offers lessons for aspiring cyber armies. The theft of advanced malware facilitates a similar shortcut to increased power on digital national security terrain. Computer code written by the Great Powers, including the United States, Russia, China, and Israel, can be acquired, reverse-engineered, and re-weaponized by small nations and even non-state actors.

Malware is a weapon unlike old-fashioned tanks and planes, and it is not necessary to break into a top-secret malware vault to steal it. Rather, compiled and fully-functioning cyber weapons can be found every day, by a careful observer, within network traffic and even on most email servers. And just as with Aladdin's magic lamp, these tools can be quickly repurposed for new operations, entirely distinct from what the malware was originally intended to do. Such malware theft can save thousands of hours of time and effort.

When Sir Isaac Newton said, "if I have seen further, it is by standing on ye shoulders of giants," [1] he was also presaging this phenomenon. Indeed, not just malware but all of today's software benefits from the millions of coders and hackers who came before. Precious little code today is written entirely from scratch. Instead, existing code is customized and/or has new features added to it. And this is only one example of the way in which IT has changed both the nature of power and the way in which power is transferred between people, organizations, and nations. This is true not only for source code, but also in the case of malware samples, where only access to executable code is available.

We know for a fact that malware re-weaponization is possible because we often see it within academic research[1] [2] [3] and in capture-the-flag (CTF) hacker competitions [4]. However, we have also seen reflections of it in real-world computer network operations by nation-states [5] [6]. Cyber actors and campaigns with names like DarkHotel, Lazarus, and TigerMilk have been seen throughout Asia, reusing attack code such as NetTraveler and Decafett in ways that also appear to incorporate false flags intended to cast blame on others during cyber operations [7].

One of the most prominent recent cases of malware source code theft involved the U.S. National Security Agency (NSA), from which code was allegedly stolen and released by the "Shadow Brokers" via the website *Wikileaks* in 2016. Reportedly, an NSA exploit named EternalBlue was leveraged in May 2017 to facilitate the WannaCry ransomware attack that targeted Windows computers and demanded Bitcoin payments. A month later, EternalBlue was used again to propagate the Petya ransomware, primarily against Ukraine. In March 2017, the Shadow Brokers also released malware allegedly developed by the CIA, again via *Wikileaks* [8].

What is a "cyber weapon"? To be sure, this term has been abused and exaggerated by analysts, journalists, and politicians, even when describing some well-known case studies [9]. And strangely, in some long-standing international conflicts, there seem to have been no known examples of cyber-attacks at all [10]. Part of the challenge in defining cyber-attacks and "cyber war" is the novelty of this new conflict domain.

1 The Bao paper cited here discusses an "automatic system" for identifying and replacing outer shellcode. Our discussion in this paper goes deeper and examines the escalation of privilege exploits, as well as a C2 replacement technique that appears perfect for false flag attacks.

On March 23, 2018, noted security researcher "The Grugq" explored this question in depth during a Black Hat conference keynote entitled, "A Short Course in Cyber Warfare." The Grugq referred to "Cyber" as the "5th Domain" of warfare, which is "literally a new dimension" and "much more complicated than anything we know." He explained that cyber-attacks comprise "Active," "Passive," "Physical," and "Cognitive" elements that can be employed in unique ways every time, making the next cyber-attack painfully hard to predict – and sometimes even to understand.[2]

For the purposes of this paper, the authors consider that a cyber-attack can be any information-based or kinetic operation designed to compromise the confidentiality, integrity, or availability of an IT system. In a national security context, such an operation must cause sufficient harm that it rises to the attention of national decision makers. It is this latter criterion that contributes to the definition controversy, as a final determination is subjective and open to political or business opportunism; however, this is a problem that certainly predates the Internet. Finally, the authors share the opinion that the malware sample analysed in this paper more than meets the requirement for a cyber weapon, as it contains two rare "zero-day" exploits and is specifically designed to give an attacker full remote-access to a target computer.

Here is what current U.S. policy states about "computer network operations": "Cyberspace is the most affordable domain through which to attack the United States. Viruses, malicious code, and training are readily available over the Internet at no cost. Adversaries can develop, edit, and reuse current tools for network attacks." [11].

The concept of malware theft via executable code manipulation (i.e. no access to source code) has also been addressed directly. In an August 2017 speech to a U.S. Department of Defense Intelligence Information Systems (DoDIIS) conference, Defense Intelligence Agency (DIA) Director Lt Gen Vincent Stewart said, "Once we've isolated malware, I want to reengineer it and prep to use it against the same adversary who sought to use it against us." [12].

Within the context of NATO, there is ample evidence that computer network operations have already risen to the highest level of importance. In 2016, NATO promised to defend allied cyberspace as it has land, sea, and air since the end of World War II. Further, it is now officially integrating cyber operations into its military plans [13] with the explicit goal of trying to deter cyber-attacks like those that have occurred in Estonia, Georgia, Ukraine, and the United States [14] [15].

The theft and re-weaponization of malware samples, in which hackers steal each other's executable code, swap existing payloads for custom munitions, and/or

2 As an example of an "Active" cyber-attack, The Grugq cited Israel's manipulation of the Palestine Liberation Organization's online financial resources; for "Passive" he cited China's "Operation Aurora" vs. Google in 2009; for "Physical" he cited Stuxnet; and "Cognitive" includes the doxing of the U.S. Democratic National Committee in 2016.

replace its command-and-control (C2) functionality, will increase the number of actors, attacks, and complexities on the cyber battlefield, and will negatively impact deterrence, diplomacy, and arms control in cyberspace.

This paper is divided into two primary sections: 1) a description of the technical aspects of malware re-weaponization, and 2) an exploration of its strategic implications.

2. MALWARE RE-WEAPONIZATION: TECHNICAL ASPECTS

In this section, the authors will examine the first part of their argument: that malware analysis is not "rocket science" and that executable code of any type can be captured, reverse-engineered, and repurposed with relative speed and ease. We will look at a genuine malware sample that was detected on a live network in 2017.[3] We believe that this malicious program was used by a nation-state with the specific intent of breaching a well-defended computer network. By any measure, it is advanced code, in part due to the fact that the program leverages no fewer than two "zero-day" exploits.[4]

The key takeaway from this short analysis is that the most technically challenging part of a cyber-attack's lifecycle – its vulnerability discovery and exploit development – can simply be stolen from another cyber actor. A malware thief (or cyber army) can then reconfigure and repurpose the code, adding unique functionality and/or control data, and then launch a high-grade cyber weapon in any direction they choose.

FIGURE 1. RUSSIAN DOLL [16]

3 The authors do not go into sufficient detail to allow the reader to create a live weapon. Specific technical details such as exact byte offsets are omitted.

4 "Zero-day" exploits target computer vulnerabilities that are yet unknown to software makers and security researchers; an exploit ceases to be a zero-day once specific patches are available.

A. Malware and its Russian doll design

Computer programs, including malware, are characterized by a layered structure that can be compared to a Russian matryoshka doll. With malware, most of the layers form a benign skeletal structure, while others (some of which can be hidden or encrypted) are designed to subvert computer security, hijack communications, or steal data.

1. Human layer
    - The outermost layer is that which humans see and understand, such as a Microsoft (MS) Office document. Our sample was an MS Word file sent via email. For an infection to begin, the email recipient simply had to open the attached file which had been expertly crafted by a phishing specialist.
2. Image file
    - Once opened, the MS file loaded an Encapsulated PostScript (EPS) image file that contained hidden, encrypted computer instructions in hexadecimal format[5] [17].
3. Shellcode
    - The decrypted code exploited a vulnerability in the Office EPS engine CVE-2017-0261 and executed shellcode that was embedded within the EPS file in order to open a command window through which an attacker could try to access the target computer.
4. Dropper
    - The shellcode was obfuscated (packed) and contained a Portable Executable (PE) file to be launched on the victim's computer. The executable file performed privilege escalation (CVE-2017-0263, individual exploits for 32- or 64-bit OS) and wrote a payload executable to disk.[6]
5. Payload
    - Once sufficient privileges were gained on the target computer, a "payload" was run, which was a fully-fledged remote administration tool that could perform a range of malicious actions such as stealing, blocking, and/or manipulating data. In our sample, the payload had been encrypted and compressed as an additional way to delay and complicate malware analysis.
6. Command-and-Control (C2)
    - After successful installation, the malware tried to "phone home" to a malicious C2 domain somewhere on the Internet in an attempt to report for duty, seek updates, and await further instructions. These communications were encrypted to help protect them from the prying eyes of network defenders.

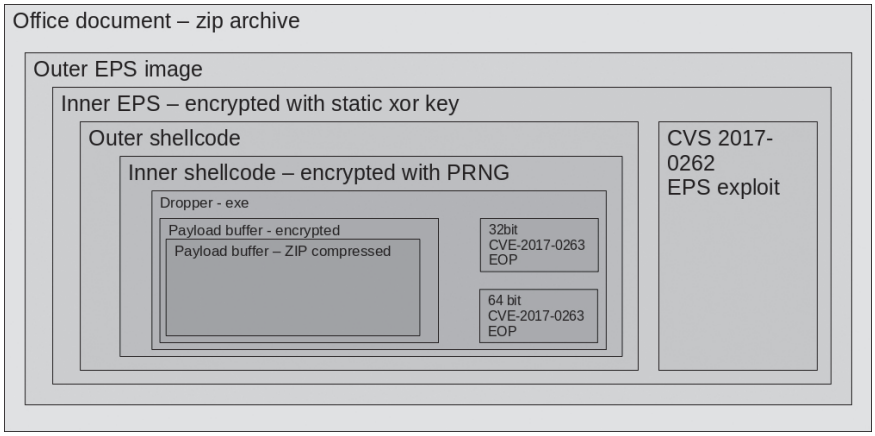
This level of malware analysis is not difficult and is available to any nation. Powerful tools such as code disassemblers and debuggers can perform decryption, de-

5 Researchers recently reported that multiple online threat actors, including Russian cyber espionage groups, have been leveraging EPS files and zero-days against European diplomatic and military entities.

6 These exploits took advantage of Common Vulnerability and Exposure (CVE) 2017-0263.

obfuscation, and unpacking of malware samples. In our case study, we employed numerous techniques. Some aspects of the design, such as the ".zip" algorithm and the "XOR cipher", are well-known to most malware researchers. Others, such as a string obfuscation algorithm for the C2, were custom-made by the malware's author, and required in-depth reverse-engineering.[7]

FIGURE 2. MALWARE SAMPLE ARCHITECTURE



B. Re-weaponization

Malware dissection at this level of detail already yields sufficient understanding for redesign and re-weaponization purposes. This section describes two ways to re-weaponize malware: 1) C2 replacement, and 2) payload replacement. Once either modification is performed, the malware thief simply reverses the steps taken in the malware's analysis, layer-by-layer, for the entire software package – just like a Russian doll.

The authors successfully tested both C2 replacement and payload replacement on this sample. They also wrote user-friendly command-line-interface scripts whereby even non-technical personnel, without any reverse-engineering knowledge, could perform the entire process.

1) Command and Control (C2) replacement

The quickest way to re-weaponize a malware sample is simply to replace its C2 components, such as by giving it a new domain that is under the malware thief's control. In fact, malware authors often reuse C2 architectures over time, even for

7 This effort required knowledge of the C programming language, as well as some luck. For example, one algorithm was symmetric, i.e. encrypt = decrypt. Asymmetric encryption could be defeated as well, but we would need to use a new encryption key and therefore the re-weaponized sample would be different from the original.

different exploits and malware campaigns. This typically serves to simplify ongoing operations which can grow in complexity over time. However, this characteristic also helps cyber defenders and malware thieves to analyse and reverse engineer how an attacker's C2 architecture works, both tactically and strategically.

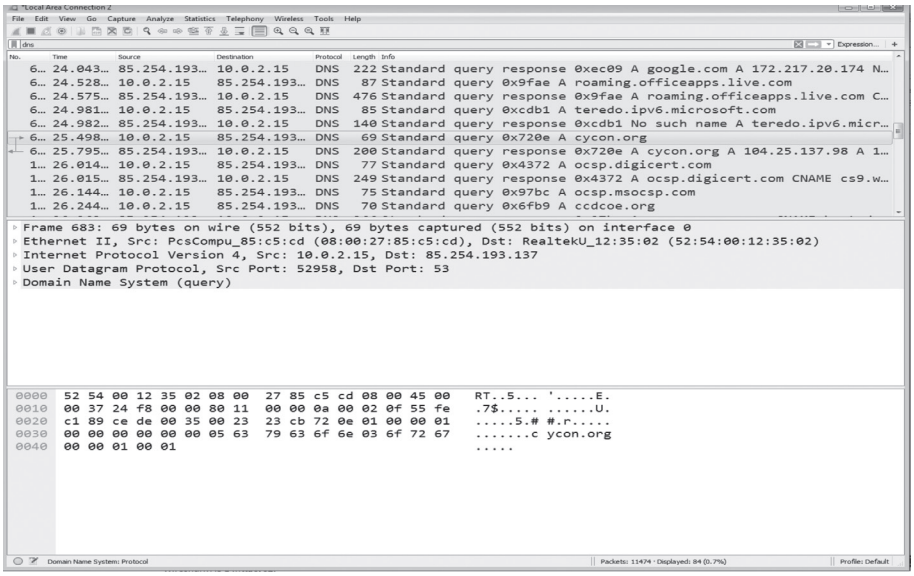
Replacing the C2 requires an intermediate level of technical expertise in software coding, reverse engineering, and network communications. But with the aid of disassembler software, this task can be accomplished relatively quickly, even by a small team or a lone expert. There can be technical limitations, such as with the length of the domain name. However, in practice, such limitations are easily overcome with some level of flexibility and creativity on the part of the malware thief.[8]

Finally, C2 replacement offers malware thieves an additional, tantalizing opportunity: the possibility of running easy false-flag operations. First, a re-weaponized malware sample is virtually indistinguishable from the original. Second, the malware thief can use the same service providers (including certificate issuers, hosters, DNS registrars, etc.) to make a new operation simply blend in with the campaign that the original attacker was already running, providing instant anonymity, or at least plausible deniability.

In Figure 3, below, the authors have written a small (120 lines of code) script to demonstrate the simplicity of C2 replacement. Here, there is just one command line parameter: the new C2 domain (cycon.org). All the necessary steps to replace the C2 domain in the malicious EPS file have been automated in an easy-to-use script. Running "python changeCnC.py cycon\.org [epsOutputFile" produces a malicious EPS file that can be included in a Word document. Once the malicious Word document is opened, malware infects the computer and connects to the modified C2 domain (cycon.org, as seen in the example screenshot). The primary challenge regarding C2 replacement is that one needs to reverse-engineer the C2 communication protocol and write server-side software to support this protocol.

8 For example, there are many ways to generate a short domain name, and to verify that it works, before an attack is launched.

FIGURE 3. C2 REPLACEMENT TO CYCON.ORG



2) Payload replacement

A second option for a would-be malware thief is to replace the payload with a tailored munition of their choice. For many scenarios, this is in fact the preferred option for a malware thief, such as:

1. when the thief already possesses custom agent and server software;
2. time constraints do not allow for C2 reverse-engineering; or
3. a proposed operation has easily achievable objectives such as wiping all data on the victim's machines.

Payload replacement is more invasive than C2 replacement and requires more malware expertise. As with C2 replacement, there can be some technical limitations, such as payload size. However, these can also be overcome with some flexibility and creativity after which the attacker can download additional malware modules via the Internet.

3. STRATEGIC IMPACT

In the previous section, the authors established that, even with limited time and expertise, a malware thief can reverse-engineer advanced malware, replace its C2 architecture, or replace its payload with a tailored munition, and launch an entirely new attack. In this section, we will explore the ramifications of this phenomenon for cyber defenders and for national security decision-makers[9] [18]. We will cover six strategic consequences in order from the logically most urgent and compelling to address to the least:

1. Proliferation
2. Attribution
3. Fog of War
4. False Flags
5. Diplomacy
6. Miscalculation

A. Proliferation

The first and most obvious challenge posed by malware re-weaponization is proliferation. Arms control, as a discipline, seeks to reduce the size of military arsenals that are capable of inflicting harm on humanity. But recycling malware means that the same vulnerabilities and exploits can be used by Country A against Country B, Country C against Country D, Country E against Country F, and so on. Furthermore, smaller nations and even non-state actors will sometimes be able to employ truly world-class digital weapons that would have been almost impossible for them to develop on their own.

So far, the cyber battlefield has seemingly been dominated by the Great Powers, such as the United States, Russia, and China, as well as regional powers with ongoing conflicts like Israel, Iran, and North Korea. Further, one experienced national security and cyber security specialist, James Lewis, recently argued that non-state actors are simply incapable of launching "massive and damaging" cyber-attacks [19]. But we suspect that most governments are, at the very least, leveraging computer network operations for cyber espionage in support of their core national security interests. We contend that malware theft and re-weaponization will only make this more common.

9 The Leitzel paper cited here, "Cyber Ricochet: Risk Management and Cyberspace Operations," uses the phrase "cyber ricochet" to denote denial-of-service attacks where the attacker does not directly communicate with the target but instead sends packets to intermediate nodes with spoofed source/destination addresses. The authors of this paper feel that the term "cyber ricochet", along with the label "reflection attack" which is used to describe a common hacker technique, imply that the malware thief is not directly controlling the operation and that an attack with unexpected consequences could result. However, when the payload or C2 infrastructure is wholly replaced, as we describe here, the attacker is in full control.

Above all, re-weaponization can save an aspiring cyber power significant time and money. IT and hacker talent are expensive. A credible cyber-attack program requires software developers, vulnerability analysts, exploit developers, malware testers, bot herders, and much more. In 2010, noted hacker and former NSA employee Charlie Miller told a CyCon audience that an effective cyber army would cost about $45 million per year with almost one-quarter of that sum spent on vulnerability analysts and exploit developers [20]. Thus, malware reuse offers a substantial reduction in cost for the most technically challenging parts of any operation: vulnerability discovery and exploit development.

B. Attribution

Increased cyber weapons proliferation means that there will be more armies on the cyber battlefield which in turn will increase the challenge of attribution. The digital battlefield has always been difficult for humans to see, understand, and contextualize. And three of the primary goals of a cyber-attacker are stealth, anonymity, or plausible deniability. Most cyber-attacks are closer to a covert operation than a traditional military operation. The laws of war state that soldiers should wear national uniforms with proper insignia, in part to bolster accountability for actions taken. However, hackers take advantage of the labyrinthine architecture of the Internet to obscure their true location.

The question of finding who is sitting at a remote keyboard is therefore fundamental to enhancing not only cyber security but also national security including deterrence, diplomacy, arms control, prosecution, and/or retaliation.[10] For computer network operations, this has been true since at least the mid-1980s.[11] Following the Cold War, and especially after the terrorist attacks of 9/11, law enforcement and counterintelligence agencies have invested considerable resources in cyber-attack attribution, but the size of the Internet and the dynamic nature of cyberspace have ensured that this will remain a vexing challenge for the foreseeable future.[12] Attribution is an art as well as a science, and a cyber-attack must usually cross a high threshold in terms of damages before sufficient resources will be allocated to its success [21].

Today, cyber defense is a professional discipline, and attribution is typically based on a wide range of observable tactics, techniques, and procedures (TTP).[13] However, in many cyber-attack investigations, there has been a singular, most valuable attribution

10 For example, in the 1990s, there were numerous cases in which the U.S. Government believed that a cyber-attack had been launched by a nation-state only to discover that it was a teenage student.

11 In the 1980s, Cliff Stoll, a system administrator at the University of California, Berkeley, spent a year tracking likely Russia-backed hackers who were targeting U.S. national laboratories, a tale recounted in *The Cuckoo's Egg*.

12 More recently, commercial firms have gotten into the attribution game. However, without the benefit of other sources of intelligence available to nation-states, such as human (HUMINT) and signals intelligence (SIGINT), they remain at higher risk of making mistakes in attribution.

13 Robust attribution relies on many pieces of evidence, including MD5 hashes, "diff" results, payloads, IP addresses, C2 infrastructure, domain names, digital certificates, network searches, exfiltrated data, source code, time zones, algorithms, encryption, current events, and more.

indicator: the malware "signature". Cyber actors have traditionally been associated with particular "families" of malware. Malware theft and re-weaponization therefore threatens to wreak havoc on the attribution process as we know it if an increasing number of players are simply using the same hacker tools that tend to be tightly controlled by their creator, and only accessible to others by malware reuse.

C. Fog of War

If already-challenging attribution becomes harder, national security decision-making will suffer from a thicker "fog of war". Sun Tzu famously wrote that "all warfare is based on deception" [22], but in the age of cyberwar, this dictum has never been more true. The problem is exacerbated by the fact that so many cyber-attacks take place during peacetime, either as cyber espionage or preparation of the battlespace for some future war that may never take place. Thus, in many ways, what we call "cyberwar" has no beginning – and no end.

The risks that cyber-attacks pose to our national critical infrastructures is high. Their integrity rests on the proper functioning of IT. This is true for everything from electricity to elections. Examples abound: in 2007, Syrian air defense personnel were apparently blinded by a cyber-attack that preceded an assault by Israeli warplanes; in 2015, foreign hackers are believed to have turned out the lights in Western Ukraine; and in 2016, Russian hackers were blamed for interfering in the U.S. Presidential election.

Malware theft and re-weaponization will increase the fog of war precisely because it increases weapons proliferation and hinders attack attribution. If all nations have access to roughly the same arsenal of vulnerabilities and exploits, who is to say that a third party is not playing *agent provocateur* in an ongoing conflict between two other nations? And how does any nation know when its cybersecurity has been compromised to the point that a traditional military invasion – or a coup d'état – is imminent? The chances for misunderstanding and miscalculation in cyberspace loom large indeed, especially in a conflict domain where time is of the essence.[14]

D. False Flags

Potential cyber-attackers know that the fog of war is thicker than ever. This fact will tempt many of them to engage in "false flag" operations that involve an effort to pin the blame on a third party. Such tactics long preceded the Internet, as pirate ships used to hoist false flags in an effort to prevent their targets from readying their defenses or evading the threat [23]. Modern spies also carry counterfeit passports, wear disguises, and lie about their true intentions.

14 Especially considering that the latest craze in both cyber-attack and defense is artificial intelligence (AI).

Malware theft and re-weaponization will tempt national-level decision-makers to engage in this type of behavior across the open Internet. False flag operations can be tricky to run as there are so many details to get right and so many ways that an operation can go wrong. But in cyberspace, the chances of success are higher, and the penalty for getting caught less severe than for a traditional military or intelligence operation. For most cyber operations, anonymity is not required, as plausible deniability will suffice.

Cyberspace is vast, and growing more crowded by the day, with students, soldiers, spies, and statesmen all living and working in the same space. There are 193 sovereign member states of the U.N., but there are 255 Internet country code top-level domains (ccTLD)[15]. This gives cyber-attackers the chance to be whomever they want, and suggests that malware reuse will increase the number of false flag political and military operations we see.

E. Diplomacy

If malware reuse is so helpful from an attacker's perspective, those who would seek to counter these advantages – law enforcement, counterintelligence, and diplomats – will have a more arduous road before them. Within the realm of international relations, the management of negotiations, treaties, and tension fall under the rubric of diplomacy. However, the rise of the Internet and cyberspace has complicated our understanding of both national security and diplomacy. There is only one Internet, and one cyberspace, and all nations are struggling to retain their traditional concepts of national sovereignty and law enforcement jurisdiction within it.

In 2018, diplomatic tensions over information security could hardly be higher. In cyber espionage, there are continuing reverberations over the Snowden revelations.[16] In propaganda, Russian interference in the U.S. electoral process has led to efforts throughout Europe to protect social media from information operations emanating from Moscow. And in nuclear diplomacy, cyber-attacks have been used by both sides on the Korean peninsula to improve their odds of victory in a real war.

Cyberwar is of special significance to diplomats for four reasons. First, cyber-attacks typically fall below the threshold of the use of force, so will be publicly addressed by diplomats more often than by soldiers. Second, most cyberwar occurs in peacetime when diplomacy takes priority over military operations. Third, diplomats are prime targets of an adversary's cyber espionage and influence operations. Fourth, alliance members risk getting dragged into a cyber conflict which they did not approve or even know about.

15 Internet country code top-level domains (ccTLD) encompass not only countries but also dependent territories.

16 For example, governments in Europe and South America have discussed building a new undersea cable in the Atlantic Ocean that could avoid direct digital contact with the United States.

Success or failure in diplomacy can have life-or-death consequences. Malware theft and re-weaponization will complicate cyber-related diplomacy, because of the expected rise in the number of actors, frequency of attacks, and the level of complexity of many cyber operations.

F. Miscalculation

History is littered with national security-related mistakes, from invading Russia to bombing Pearl Harbor, made by those who trusted in hope. It is human nature to be overly optimistic. And the theft of world-class malware is no different, carrying as it does risks for any malware thief. Attribution is difficult, but ultimately not impossible. It is easy to imagine that smaller nations, without sufficient political and military strength, will use such a weapon rashly and prematurely, and suffer disproportionate retaliation, in what could be a miscalculation of strategic proportions.

The fact that computer network operations are often time-sensitive only adds to this risk. When an attacker is able to pair an exploit (even a zero-day) with a discovered vulnerability, it is understood that the window of opportunity will not be open forever. A system administrator or software company can update, patch, or harden the target network, operating system, or application at any time. Malware signatures are constantly updated. And a malware thief has the added pressure of knowing that at least one other party knows about the exploit and vulnerability.

Even the possession of powerful malware does not mean that an attacker can properly execute all facets of a complex computer network operation. Part of it they may get right and others wrong. Hackers are routinely caught during any phase of a cyber-attack, from reconnaissance, to lateral movement on a network, during data exfiltration, and so on – sometimes even long after an attack is over. Incident response is always improving, and if done correctly, it will incorporate traditional intelligence analysis sources and methods as part of its attribution determination.

A final consideration involves stolen malware that has been backdoored, trojaned, or watermarked (potentially with malware theft in mind). Unless a hacker has written a computer program from scratch, it is hard to know whether it contains undiscovered, hidden functionality. For example, in 2013, the Syrian government allegedly targeted non-governmental organizations in Syria by encouraging them via social media to download Freegate, a common Virtual Private Network (VPN) client used to circumvent censorship. The Syrian government had reportedly trojaned this version of Freegate, precisely to target domestic opposition [24]. Thus, the desire for a quick, cheap cyber-attack can lead a malware thief into a trap.

4. CONCLUSIONS

For Aladdin, the acquisition of a magic lamp brought both benefits and risks. The theft and re-weaponization of malware is no different. Smaller nations, and even non-state actors, can obtain powerful digital weapons almost for free. As a result, there will be more armies on the cyber battlefield, more cyber-attacks, and a higher overall level of complexity for cyber defense. This phenomenon will have ramifications for weapons proliferation, attack attribution, the fog of war, false flag operations, international diplomacy, and strategic miscalculation.

If a malware thief asks too much of the magic lamp, however, there may be serious repercussions and unintended consequences. All cyber thieves must ask themselves whether they have the traditional political and military might to absorb a potential response. In this light, reliable attribution might still tend toward traditionally strong military powers – states that in any case may be less concerned with unforeseen consequences.

In terms of mitigating the potential impact of malware theft and re-weaponization, governments are likely to consider a wide range of options, including enhanced vulnerability disclosure,[17] watermarking digital weapons to keep closer track of them, the use of blockchain to enhance attribution, and even the signing of non-aggression pacts for cyberspace.[18] More research is needed on mitigation strategies.

In the longer term, it is possible that an increased awareness of this phenomenon will slow down the current pace of cyber operations worldwide, so that nations can better safeguard their code and operations. Potentially, this will serve to decelerate the prevailing level of conflict and instability in cyberspace, since every nation is now home to an abundance of cyber vulnerabilities. Advanced cyber powers might be wise to consider more carefully the potential fallout from approving reckless digital operations so that they do not lose control of the magic lamp.

5. REFERENCES

[1] I. Newton, "Letter from Sir Isaac Newton to Robert Hooke (1675)," Historical Society of Pennsylvania, 2017. Available: https://discover.hsp.org/Record/dc-9792/Details [Accessed March 28, 2018].

[2] R. W. Y. S. D. B. T Bao, "Your Exploit is Mine: Automatic Shellcode Transplant for Remote Exploits," IEEE Symposium on Security and Privacy, San Jose, 2017. Available: https://www.ieee-security.org/TC/SP2017/papers/579.pdf [Accessed March 28, 2018].

[3] Y. S. R. W. C. K. G. V. D. B. Tiffany Bao, "How Shall We Play a Game? A Game-theoretical Model for Cyber-warfare Games," Carnegie Mellon University, p. 1. Available: https://users.ece.cmu.edu/~youzhib/paper/bao2017csf.pdf [Accessed March 28, 2018].

17 Cyber commands already weigh the operational value of vulnerabilities and exploits against their national exposure to them.

18 There might be voluntary limits on cyber espionage, which is understood to be a natural precursor to cyber-attack.

[4] W. K. J. Yam, "Strategies used in capture-the-flag events contributing to team performance," Naval Postgraduate School, March 2016, pp. 2-3. Available: https://calhoun.nps.edu/bitstream/handle/10945/48498/16Mar_Yam_Jerel.pdf?sequence=1&isAllowed=y [Accessed March 28, 2018].
[5] J. Cox, "The CIA Allegedly 'Borrows' Code From Public Malware Samples," *Motherboard*, March 7, 2017. Available: https://motherboard.vice.com/en_us/article/3dyd53/the-cia-allegedly-borrows-code-from-public-malware-samples [Accessed March 28, 2018].
[6] G.-S. C. R. Juan Andrés, "Walking in Your Enemy's Shadow: When Fourth Party Collection Becomes Attribution Hell," in *Virus Bulletin*, Madrid, 2017. Available: https://cdn.securelist.com/files/2017/10/Guerrero-Saade-Raiu-VB2017.pdf [Accessed March 28, 2018].
[7] K. Zetter, "Masquerading Hackers are Forcing a Rethink of How Attacks are Traced," *The Intercept*, October 4, 2017. Available: https://theintercept.com/2017/10/04/masquerading-hackers-are-forcing-a-rethink-of-how-attacks-are-traced/ [Accessed March 28, 2018].
[8] M. R. A. W. L. Scott Shane, "WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents," *New York Times*, March 7, 2017. Available: https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html [Accessed March 28, 2018].
[9] M. D. Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better," in *4th International Conference on Cyber Conflict*, NATO CCD COE, Tallinn, 2012. Available: https://ccdcoe.org/publications/2012proceedings/2_6_Dunn%20Cavelty_TheMilitarisationOfCyberspace.pdf [Accessed March 28, 2018].
[10] R. C. M. Brandon Valeriano, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, New York, NY: Oxford University Press, 2015, p. 2. Available: http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/cyber_war_versus_book_review_itp.pdf [Accessed March 28, 2018].
[11] "Strategic Cyberspace Operations Guide," United States Army War College, June 1, 2016, p. 7. Available: https://info.publicintelligence.net/USArmy-StrategicCO.pdf [Accessed March 28, 2018].
[12] I. Thomson, "US Military Spies: We'll Capture Enemy Malware, Tweak it, Lob it Right Back at Our Adversaries," *The Register*, 15 Aug 2017. Available: https://www.theregister.co.uk/2017/08/15/us_government_wants_to_reverseengineer_malware_to_fight_back/ [Accessed March 28, 2018].
[13] NATO, "NATO Defence Ministers Agree to Adapt Command Structure, Boost Afghanistan Troop Levels," November 9, 2017. [Online]. Available: https://www.nato.int/cps/en/natohq/news_148722.htm. [Accessed December 2017].
[14] T. E. Ricks, "NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons," *Foreign Policy*, December 7, 2017. Available: http://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/ [Accessed March 28, 2018].
[15] C. Bing, "Russia-linked Hackers Impersonate NATO in Attempt to Hack Romanian Government," *Cyberscoop*, May 11, 2017. Available: https://www.cyberscoop.com/dnc-hackers-impersonated-nato-attempt-hack-romanian-government/ [Accessed March 28, 2018].
[16] W. Commons, "Floral matryoshka set 2 smallest doll nested," [Online]. Available: https://commons.wikimedia.org/wiki/File:Floral_matryoshka_set_2_smallest_doll_nested.JPG. [Accessed December 2017].
[17] A. L. A. B. B. R. D. K. G. M. Genwei Jiang, "EPS Processing Zero-Days Exploited by Multiple Threat Actors," FireEye, May 9, 2017. Available: https://www.fireeye.com/blog/threat-research/2017/05/eps-processing-zero-days.html [Accessed March 28, 2018].
[18] B. Leitzel, "Cyber Ricochet: Risk Management and Cyberspace Operations," Center for Strategic Leadership, U.S. Army War College, 2012. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a568619.pdf [Accessed March 28, 2018].
[19] J. Lewis, "Fighting the Wrong Enemy, aka the Stalemate in Cybersecurity," *The Cipher Brief*, November 26, 2017. [Online]. Available: https://www.thecipherbrief.com/column_article/fighting-the-wrong-enemy-aka-the-stalemate-in-cybersecurity. [Accessed March 9, 2018].
[20] C. Miller, "Kim Jong-Il and Me: How to Build a Cyber Army to Defeat the U.S.," oral presentation at *CyCon and DEF CON 18*, Tallinn and Las Vegas, 2010.
[21] B. B. Thomas Rid, "Attributing Cyber Attacks," *The Journal of Strategic Studies*, vol. 38, no. 1–2, p. 4–37, 2015.
[22] S. Tzu, "Wikiquote," Creative Commons, [Online]. Available: https://en.wikiquote.org/wiki/Sun_Tzu [Accessed March 28, 2018].
[23] L. deHaven-Smith, *Conspiracy Theory in America*, University of Texas Press, Austin, 2013, p. 225.
[24] M. M.-B. John Scott-Railton, "A Call to Harm: New Malware Attacks Target the Syrian Opposition," The Citizen Lab, Toronto, June 2013. Available: https://citizenlab.ca/2013/06/a-call-to-harm/ [Accessed March 9, 2018].