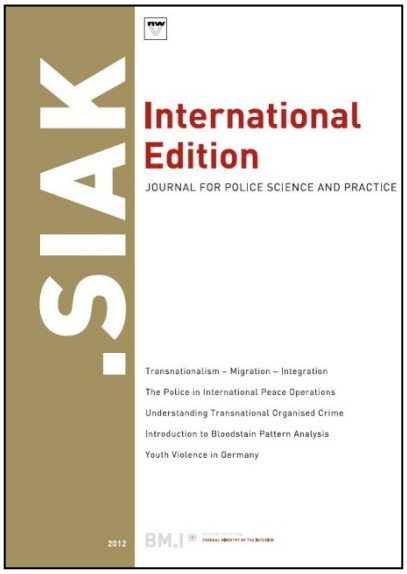
.SIAK REPUBLIC OF AUSTRIA
FEDERAL MINISTRY OF THE INTERIOR
SICHERHEITSAKADEMIE

.SIAK-Journal – Journal for Police Science and Practice



Braganca, Maschenka (2014):

Hunt for Red October. The new face of cyber espionage

SIAK-Journal − Journal for Police Science and Practice (International Edition Vol. 4), 87-95.

doi: 10.7396/IE_2014_H

Please cite this articel as follows:

Braganca, Maschenka (2014). Hunt for Red October. The new face of cyber espionage, SIAK-Journal − Journal for Police Science and Practice (International Edition Vol. 4), 87-95, Online: http://dx.doi.org/10.7396/IE_2014_H.

published online: 8/2014

Hunt for Red October

The new face of cyber espionage

Operation Red October – the newly discovered cyber espionage campaign that has targeted a range of diplomatic facilities, defense companies, and energy firms, especially in Eastern Europe but also around the globe – may mark an evolution of the cyber black market. In October of the past year computer security researchers discovered a type of malware that appears to have been part of a widespread cyber espionage campaign that outplays major operations such as the notorious Flame Virus that was used in a very targeted manner to spy on Middle Eastern countries. The intrusions in the Red October Campaign remained unnoticed for more than five years and might still be looming in the dark at some organizations. The discovery was made public only in October 2012 after the month-long work of a Russian security company that found the malware used to infiltrate computer systems in the recent campaign. They also managed to take out large parts of the malware infrastructure, and subsequently did in-depth analysis in order to work against the perpetrators and draw some conclusions about motivation and origins. This article looks at the details of Operation Red October, analyzes its nature, impact and ways, in which the trade form of espionage is changing with the evolution of a new threat environment.

MASCHENKA BRAGANCA,
political scientist with a focus on foreign and security policy.

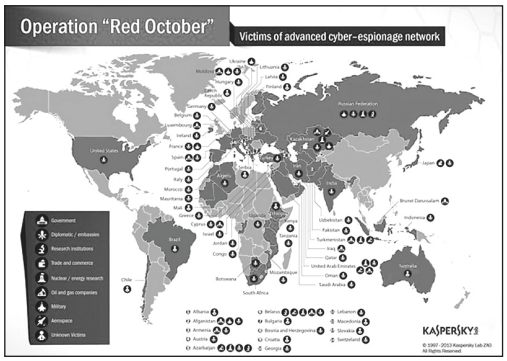
OPERATION RED OCTOBER – CYBER ESPIONAGE CAMPAIGN

During the past five years, the campaign that has come to be known as "Operation Red October" has successfully infiltrated computer networks at more than 350 diplomatic, governmental and scientific research organizations, gathering data and intelligence from mobile devices, computer systems as well as network equipment. The places targeted were spread around the globe with a significant prevalence in Eastern Europe and former Soviet Republics. Targets include trade and commerce organizations, nuclear and energy research groups, oil and gas companies, as well as the aerospace industry. They also include a handful of non-US diplomatic organizations inside the United States. The Red October malware network is considered one of the most advanced online espionage operations that has been discovered to date. The researchers from Kaspersky Lab named it "Red October" – shortened to "Rocra" – inspired by the almost noiseless submarine from the eponymous Tom Clancy novel. The name seems to be a fitting analogy – a digital submarine lurking for more than five years, searching for classified and sensitive information. There

is even reason to believe that some of the victims might not even have realized the data theft yet.

One of the targets has apparently been the Russian Embassy in the United States, where tens of thousands of documents, probably including classified reports to the foreign ministry in Moscow, have reportedly fallen into the hands of cyber spies. Besides exfiltration of documents, Rocra has also been used to steal encrypted files and decryption keys used by the European Union and NATO (Nakashima 2013). It is possible that a total of several terabytes of data were stolen. The targets very clearly indicate an interest in geopolitically significant information and government secrets.

Source: Kaspersky Lab 2013



Graphic 1: Operation Red October, geographical distribution of victims

ATTACK ARCHITECTURE AND VECTORS

Kaspersky Lab's researchers have analyzed the operation in lengthy detail, with a focus on the modules used for attack and data exfiltration comprised of malicious extensions, info-stealing modules and backdoor Trojans (Kaspersky Lab 2013). They could figure out how the different stages of the attack were put into action as well as the malware family used in the attacks, which was dubbed "Sputnik". Kaspersky Lab used a sinkhole[1] strategy to understand what was happening. This involved setting up several victims around the world

Source: Kaspersky Lab 2013

Country	Infections
Russian Federation	35
Kazakhstan	21
Azerbaijan	15
Belgium	15
India	14
Afghanistan	10
Armenia	10
Iran; Islamic Republic of	7
Turkmenistan	7
Ukraine	6
United States	6
Vietnam	6
Belarus	5
Greece	5
Italy	5
Morocco	5
Pakistan	5
Switzerland	5
Uganda	5
United Arab Emirates	5

Table 1: List of countries with most infections

and monitoring how the attackers handled them over the course of several months, which allowed them to collect hundreds of attack modules and tools.

One major discovery resulting from this investigation was that in order to control the network of infected machines, the attackers had created more than 60 domain names and several server hosting locations in different countries (many of them in Germany and Russia). Kaspersky Lab's analysis of Rocra's Command & Control (C&C or C2) infrastructure shows that the chain of servers was actually working as proxies in order to hide the location of the "mothership" control server. A control and command infrastructure is the backbone of any attack of this kind, and instead of using a single command and control server it utilizes an embedded command and control approach, thus avoiding any single point of failure.[2]

Though control and command servers are sometimes key to some of the most carefully constructed attacks, or what are called "advanced persistent threats"[3], these attacks are typically remotely orchestrated

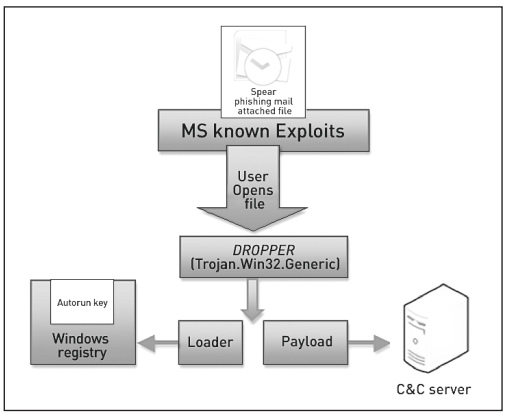
via C&C communications between the infiltrated systems and the attackers themselves. Typically, malware will call back to these servers for additional downloads or instructions, and can be used by attackers to access the infected system. Traffic for C&C servers in persistent attacks is very low (compared to botnets) and often hard to locate. Attackers change and redirect addresses, use legitimate sites, and even set up C&C servers inside a company's network in order to not raise suspicion.

So, in the Red October Campaign the attackers first infected the systems of the targeted organizations and created a multi-functional attack platform with different extensions and malicious files to adjust to the specific configuration of the system under attack and harvest the sought-after intelligence from them. It is unique in the sense that the type of modules used has not been identified in previous cyber espionage campaigns.

1. Infecting Victims

To infect systems, the attackers sent a targeted spear-phishing[4] email to a victim that included an attachment. This attachment was a customized Trojan dropper as can be seen in graphic 2, which basically is an exploit rigged for vulnerabilities in Microsoft Office programs (MS Word and Excel). The goal is to infect a target system with backdoor and dropper software (the so-called Sputnik).

Source: Kaspersky Lab 2013



Graphic 2: First stage of attack as the foundations are laid

2. Insert the payload that enfolds once the system is infected via multi-layered platform

- "Resurrection" module, which functions as a back-up solution in case the main piece of malware gets discovered. The way this works is that the module is embedded as a plug-in in a program such as Adobe Acrobat and allows the C&C station to regain control of the victim system, which again sends a file to the victim station (e.g., via email) that in a renewed effort activates the malware.
- Advanced cryptographic spy-modules, the main purpose of which is stealing information from different cryptographic systems such as Acid Cryptofiler used by NATO, the EU, and some EU agencies to protect sensitive information.
- Mobile devices: The malware is able to steal information from mobile devices such as smartphones but also routers and other enterprise network equipment.

All these elements showcase the careful planning behind this operation that not only has been extremely targeted but also sophisticated. The programmers made sure that the information sought after would be grasped with high certainty.

An interesting point is that the Red October campaign does not appear to be a single campaign, but, rather, a concerted effort via a series of campaigns that may have been launched at various times and targets since 2007. Also, it appears that some of the exploits have been "re-used" from different attacks, i.e., programmed by other attackers before Rocra and then re-used and adapted for that purpose[5].

Kaspersky, in the attempt to take down the operation, has sinkholed more than 60

domains being used by the malware, and found victims in 39 different countries. Around 250 different IP addresses were connected to the sinkhole, which it ran from last 2 November, 2012 to 10 January, 2013. After the sinkholing and the publication of the discovery, it was noted that the attacker's control servers were gradually being taken offline in an attempt to destroy evidence (Kaspersky Lab 2013).

ATTRIBUTION AND MOTIVATION

When it comes to the question of origin, attribution and motivation, cyberspace is a grey zone with little to no clarity. In the Red October case, from a few hints, the researchers from Kaspersky Lab deduced that there are Russian-speakers involved at least at the lowest level of the attack, the actual coding. First, based on the registration data of C&C servers and the traces left in the executables of the malware, there is strong technical evidence to indicate the attackers have Russian-speaking origins (Kaspersky Lab 2013). Second, Russian slang words keep appearing in the code, including words like "zakladka", which can mean "bookmark"[6] and "proga" meaning program. The perpetrator that actually might have ordered and planned the campaign could, however, still be someone else. The sophisticated and targeted nature of the intrusions strongly suggests that any principal would have to have the appropriate financial means. This could mean that a national government and intelligence service might have ordered it – however, it could as well be criminals looking to sell the data to a government.

What was clear is that Rocra was designed to steal data from specific targets – assigning people unique ID numbers and in some cases employing malware modules customized solely for that target. Studying this becomes difficult as researchers are not able to see the data that was stolen or recover every attack module. The techniques used, however, enabled the researchers to trace servers and IP addresses of the targets. Kaspersky Lab in this specific case used detection statistics from the Kaspersky Security Network (KSN) as well as the sinkhole analysis.

Some researchers and security experts argue that given the customized malware, massive command-and-control infrastructure, and the sheer amount of data stolen, some researchers say a nation-state has to be behind it (Alperovitch 2013). Also, the strong emphasis on diplomatic organizations points towards a nation-state as the "end customer" of the stolen information. It is just not clear, based on the technical information that has been gathered thus far, who this entire operation can be attributed to. The exploits used in the attacks are of the type used by Chinese advanced persistent threat (APT) actors, but the malware writers appear to be native Russian-speakers, according to Kaspersky's findings. Dmitri Alperovitch, Chief Technical Officer (CTO) of the newly founded security company CrowdStrike, says the attacks have all the earmarks of a nation-state sponsored initiative.

EVOLUTION OF ADVANCED AND TARGETED THREATS

Advanced Persistent Threat (APT) is the term used to describe a cybercrime category directed at business and political targets that requires a high degree of stealth over a prolonged duration of operation in order to be successful. The attack objectives therefore typically extend beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and initial goals reached. The idea is to conduct an operation without letting the victim realize what is happening or at the most confuse

him. That is what happened in the case of Stuxnet[7], where the attackers put a lot of effort into creating an elaborate side show to distract the laboratory staff at the enrichment facilities in Natanz.

Red October is exactly one of these spyware programs that are complex and costly but do not have a huge financial gain – they are designed to steal political information as opposed to Research and Development (R&D) plans, intellectual property or bank data. Red October has taken to typical nation-state intelligence gathering activities from reconnaissance to theft of secret classified information (Sweetman 2012, 72).

The nature of so-called Advanced Persistent Threats (APT) is that they are

a) advanced in that operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal but also extend to conventional intelligence-gathering techniques, and often combine multiple targeting methods and tools in order to reach the target and maintain access to it,
b) persistent in that they try to reach their objective in a "low and slow" approach, maintain long-term access to the target in order to exfiltrate data over a long period of time and make sure the objective in mind has been fulfilled and
c) a threat, which means APTs have capability and intent, the operators are skilled, motivated and well-funded (Borger 2001).

All these elements have been met at a high level by the Rocra Operation.

Kaspersky Lab claims to have never before seen an attack done with such "surgical precision" (Kaspersky Lab 2013). It is an extensive cyber espionage coup about national security secrets of certain countries. Rocra is not as sophisticated as Flame, which spread through Windows software updates, but it is described as more "elegant" (Nakashima 2013). It also does not belong to the family of Stuxnet, Duqu and Flame is also more widespread and massive than the infamous Flame cyberspying campaign, according to researchers at Kaspersky Lab.

A NEW ERA OF ESPIONAGE – WHAT DO WE LEARN FROM THIS CAMPAIGN?

What all this shows, is that there is a slow but steady shift in intelligence and espionage conduct. "The most elegant cyber attacks are a lot like the most elegant bank frauds [...] They work best when the victim doesn't even know he's been robbed"[8] (Sanger 2012, 5). Getting in and getting out again requires you to think like a bank thief casing a well-protected vault.

Intelligence is a way to enhance your understanding of a situation and thereby create a precise knowledge of your adversaries' and allies' capabilities and intentions and can also provide decision advantage vis-à-vis your adversaries (Sims/Gerber 2008). Information technology has always been important to gather intelligence on your opponents – whether to assist in war fighting, or to learn who is developing weapons of mass destruction (reconnaissance purposes). With regard to the intelligence collection process, significant revolutions occurred in the past century towards signals intelligence (SIGINT) towards a fully integrated system bringing together Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR).

The main characteristic of this (r)evolution was that technological advances brought about a large basis for intelligence that could not only be used to provide strategic warning for decision-makers, but could be directly linked to tactical operations, and therein enabled complete control of the battle space. This flow of new data also necessitated more large-scale analy-

sis, which was reflected in the creation of new offices and analytical units (Smith 2001, 40). Surveillance was then not only provided by spies on the ground (human intelligence or HUMINT) but increasingly shifted up to the air, and later space, accompanied by significant advancements in electronic surveillance technology e.g., radar[9]. The C4ISR revolution shows how capabilities have evolved not only to provide strategic or tactical reconnaissance but that the goal is to develop and apply formidable strategic capabilities to tactical efforts in increasingly more effective ways.

Space-based reconnaissance evolved as part of the revolution in strategic intelligence and subsequently, the "revolution in military affairs" (RMA), and provided the US strategic advantage during the Cold War and beyond. The basic idea of ISR (intelligence, surveillance and reconnaissance), is to utilize technological advancements for strategy, intelligence and tactics.

Cyberspace, however, is essentially a new environment – a unique ecosystem. In the 1980s and 1990s the "revolution in military affairs" recognized the role of information technology in the conduct of armed forces. But only in the last decade did the realization occur that cyberspace itself has become more than a tool (such as reconnaissance aircraft or aperture radars), but an actual environment. This is a transformation of the global (technological environment) into an artificial environment, in which new rules and power-relations are being established – an environment that state and non-state actors will engineer to suit their strategic interests (Deibert 2011). The goal is to maintain or attain strategic advantage relative to competitors.

Cyberspace is an integrated domain, where public and private, civil and military (though separate networks), national as well as foreign actors operate simultaneously. The anonymity that cyberspace provides allows for complete anonymity of transactions and content and makes attribution a difficult task. The cyber realm offers actors a space that is sheltered and vastly unregulated and therefore allows for all kinds of illicit trade. You cannot pinpoint who is behind an attack/campaign – attacks could even be "crowd sourced" by governments (Choucri/Goldsmith, 2012). Another characteristic of the networked environment is that sensitive documents that were locked in filing cabinets behind locked doors are now migrating into the cloud and embedded in social networking services that have questionable security architectures and poor data handling practices – thumb drives being inserted and circulating, disks uploading information, mobile phones sending and receiving information while roaming over different networks.

Now cyber intrusions are not only directed against governmental networks but the great majority target private corporations, which come under the purview of a national government. One of the biggest problems besides cyber crime and a problem that the FBI identifies as its number 1 criminal priority in the cyber realm, is industrial or economic espionage (Robinson 2007, 5).

However, with regard to state owned intelligence efforts, cyber espionage is "potentially the most valuable addition to spycraft since the advent of signals intelligence" (Sweetman 2012, 18). The intake can include large volumes of detailed technical information that can be disseminated with relative freedom to end-users – people designing and engineering systems. The relative freedom comes from the fact that no agents are at risk and the techniques and software used for network penetration are not designed for a long life: The presumption is that they will be detected, countered and replaced with something new.

WHAT IS BEING DONE – WHAT NEEDS TO BE DONE?

One effect of the cyber environment is that such attacks are difficult to detect a priori and an attack or intrusion – especially the more advanced and persistent kind – is often recognized only after significant damage has been done. There is a range of strategies used to protect networks, some of them more passive and reactive, whereas others are more offensive. Among them are:

- Securing hardware and software by a layered approach utilizing the most up-to-date security software (firewalls, scanners, 2-factor-authentication, penetration testing of networks, malware detection systems, and other techniques).
- Threat analysis and forensics for APTs: threat analysis is a concept often associated with security threat intelligence, where the focus is directed towards gaining knowledge of new and existing threats for the purpose of formulating defenses to mitigate them. Therefore, the cycle of prepare/analyze/identify/respond (PAIR) is a useful model to more effectively leverage these systems and data with analytical techniques to help locate and eradicate threats in the environment (Spruell/Wanner 2007, 4).[10]
- Collaboration between IT security providers, government and law enforcement entities: in the case of Rocra, Kaspersky Lab is collaborating with international organizations, law enforcement agencies and national Computer Emergency Response Teams (CERTs) of the victim states, thereby continuing the investigation and providing resources for mitigation and remediation (Kaspersky Lab 2013).
- Early warning and good counter-intelligence: effective counter-intelligence is an essential element in combating foreign technical threats. The major problem with cyber is not the actual attack with a kinetic/physical effect such as power outages but cyber espionage and exfiltration, exfiltration of information without knowledge of the victim. Part of this is due to our overarching dependence on sophisticated IT and net-centric concepts. What has been a measure of technological edge has increasingly proven to be a huge disadvantage in an adversarial environment (cf. Gosler 2008, 173–198).

To conclude, it has to be said that the threats emanating from cyberspace and the utilization for intelligence collection require a joint conceptualization of our strategic environment – physical and virtual. Virtual means might be the preferred way to go, but the objectives and motivations still remain strikingly similar. Getting in and getting out again still requires you to think like a bank thief.

[1] *The sinkoholing technique has been successfully used in the past to bring down the Zeus Trojan and associated botnet.*

[2] *Usually a group of infected computers that have been recruited for running malicious software is referred to as a "botnet". A botnet's originator can control the group and is usually referred to as the main command-and-control server (C&C server).*

[3] *APTs are longlasting sustained attacks with a high level of sophistication and a major impact on the victim system.*

[4] *Spearphishing is an attempt directed at specific individuals or companies, where information (such as usernames, passwords, credit card digits, etc.) is acquired by masquerading as a trustworthy entity in electronic communication.*

[5] *E.g., by using various embedded executables.*

[6] *Intriguingly, Kaspersky's researchers explain that in Russian, the term "Zakladka" also refers to a "microphone embedded in a brick of the embassy building", implying the bugging technique, which was an old standard method used for penetration and interception by the US and USSR/Russia for decades.*

[7] *Stuxnet is the name by which the cyber attack used to bring down Iranian uranium enrichment efforts came to be known as.*

[8] *One of the early architects of "Olympic Games" was quoted as having told David E. Sanger, when asked how Washington was making use of the new technology of offensive cyber weapons.*

[9] *The shift from air to space: a further step in the creation of far-reaching, detailed accurate and stealthy reconnaissance capabilities was the shift to the use of satellites during the Cold War. One of the reasons for this was that aircraft could be detected and tracked as well as shot down at some point and space-based systems offered some benefits by circumventing the dangers threatening aerial overflight.*

[10] *The SANS Advanced Threat Analytics Paper provides an excellent, simple and in-depth overview of identification, mitigation strategies and incident response procedures.*

Sources of information

Alperovitch, D. (2013). 'Red October' Attacks: The New Face of Cyberespionage, Dark Reading.com.

Borger, J. (2001). America's War with an invisible enemy. Guardian Online. May 8, http://www.guardian.co.uk/world/2001/may/08/worlddispatch.julianborger.

Choucri, N./Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations and global security, Bulletin of the Atomic Scientists, 70–77.

Deibert, R. (2011). Tracking the emerging arms race in cyberspace, Interview, The Bulletin of the Atomic Scientists 67 (1), 1–8.

Gosler, J. (2008). Counterintelligence: Too Narrowly Practiced, in: Sims, J. E./Gerber, B. (eds.) Vaults, Mirrors & Masks: Rediscovering US Counterintelligence, Washington D.C.

Kaspersky Lab (2013). "Red October" Diplomatic Cyber Attacks Investigation. Jan 14, http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide.

Nakashima, E. (2013). Computer Malware targets European Agencies. Washington Post, 14 Jan, http://articles.washingtonpost.com/2013-01-14/world/36323010_1_malware-flame-virus-targets.

Robinson, S. (2007). Corporate Espionage 201, SANS Institute Infosec Reading Room, http://www.sans.org/reading_room/whitepapers/engineering/corporate-espionage-201_512.

Sanger, D. (2012). Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power, Washington D.C.

Sims, J. E./Gerber, B. (eds.) (2008). Vaults, Mirrors & Masks: Rediscovering US Counterintelligence, Washington, D.C.

Smith, C. (2001). CIA's Analysis of Soviet Science and Technology, CIA's Analysis Of The Soviet Union, 1947–1991, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/cias-analysis-of-the-soviet-union-1947-1991/analysis_sANDt.pdf.

Spruell, D./Wanner R. (2007). Advanced Threat Analytics for Incident Response. SANS Institute InfoSec Reading Room, www.sans.org/.../advanced-threat-analytics-incident-response_2133.
Sweetman, B. (2012). I Spy, Aviation Week & Space Technology 174 (40), 72.

Further literature and links

Carr, J. (2012). Inside Cyber Warfare: Mapping the Cyber Underworld, Sebastopol, CA.
Clarke, R. A./Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It, New York.
INSA Report (2011). Cyber Intelligence. Setting the Landscape for an Emerging Discipline, https://images.magnetmail.net/images/clients/INSA/attach/INSA_CYBER_INTELLIGENCE_2011.pdf.
Johnson, L. (2007). Handbook of Intelligence Studies, New York.
Williams, P./Shimeall, T./Dunlevy, C. (2002). Intelligence Analysis for Internet Security, Contemporary Security Policy 23 (2), 1–38.
Cyber Statecraft Initiative of the Atlantic Council, http://www.acus.org/tags/cyber-statecraft-initiative.
International Cyber Security Protection Alliance, https://www.icspa.org/.
KillerApps – National Security in the Cyber Age (John Reeds Foreign Policy Blog), http://killerapps.foreignpolicy.com/.
NATO Cooperative Cyber Defence Centre of Excellence, https://www.ccdcoe.org/.
Zero Day – The Threat in Cyberspace. A Washington Post Special Report, http://www.washingtonpost.com/investigations/zero-day.