Revolution Hacking

by

Nikolay Koval

Chapter 6 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Nikolay Koval, head of Ukraine's Computer Emergency Response Team (CERT-UA) during the revolution, describes in Chapter 6 how cyber attacks rose in parallel with ongoing political events, in both number and severity. In 2012, hackers 'defaced' Ukrainian government websites with politically motivated digital graffiti. In 2013, network defenders discovered new and more menacing forms of malware, such as RedOctober, MiniDuke, and NetTraveler. In 2014, hacktivist groups such as CyberBerkut published stolen Ukrainian Government documents. Koval analyses in detail the most technically advanced attack investigated by CERT-UA: the May 2014 compromise of Ukraine's Central Election Commission (CEC). He closes by appealing to the Ukrainian Government to allocate greater funds to hire and retain qualified personnel.

CCDCOE

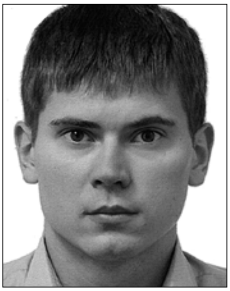
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication. Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation. Please contact publications@ccdcoe.org with any further queries.

Chapter 6

Revolution Hacking



Nikolay Koval

CyS Centrum LLC

1 Introduction: Cyber Conflict in Ukraine

During Ukraine's revolution in 2014, I served our country as the chief of its Computer Emergency Response Team (CERT-UA).[1] During my tenure, we responded to a wide variety of network security incidents. I can say with great confidence that the number and severity of cyber attacks against Ukraine rose in parallel with ongoing political events.

Before the revolution, Ukraine experienced a fairly typical array of incidents, the most frequent of which were botnet-driven[2] Distributed Denial of Service (DDoS) attacks. Often, these came in retaliation for unpopular government initiatives, such as when the authorities tried to shut down the file-sharing website www.ex.ua. By the end of 2012, some of the public's frustration was channelled into politically motivated website 'defacements' (i.e. digital graffiti) within the government's Internet Protocol (IP) space.

> *The number and severity of cyber attacks against Ukraine rose in parallel with ongoing political events.*

In 2013, we began to discover a much more serious class of malware. Network vandalism had given way to a surge in cyber espionage, for which commercial cyber security companies developed a list of colourful names: RedOctober, MiniDuke, NetTraveler, and many more.

[1] CERT-UA lies within the State Service for Special Communications and Information Protection of Ukraine.

[2] In other words, the botnets were large enough that no other amplification was needed.

Once the revolution began in February 2014, even ordinary Ukrainians became familiar with the combination of hacking and political activism, or 'hacktivism', in which the attackers seek to wage psychological war via the internet. Although many people were exhausted by the momentous political events that had shaken our country, it was hard to ignore the publication of allegedly leaked Ukrainian government documents detailing a secret, fascist government agenda. The most prominent hacktivist group was CyberBerkut,[3] and it is their most famous attack which is detailed below.

In the course of so many incident responses we learned that, with sufficient evidence, it is usually possible to understand the general nature of an attack, including who the attackers might be and what they were seeking. Timing, context, victim identity, and malware sophistication are good indicators. Cutting-edge spyware is likely to be found on the computers of senior government officials or on important network nodes within national critical infrastructure. For example, in one case, we wondered why a private sector executive had been hit, and then discovered that he had previously been a high-ranking government official.

In my opinion, CERT-UA – in collaboration with network security firms such as Kaspersky Lab, Symantec, ESET, and others – was usually able to detect, isolate, and eliminate serious threats to network security in Ukraine.

However, in the course of our work, we also discovered another problem that any enterprise today should seek to address: a fundamental lack of user understanding of cyber security. At every institution, therefore, we tried to carry out a malware 'literacy campaign' to teach employees how infections begin and how attackers can subsequently control their computers to steal documents, all via a tiny, unauthorised program that can be maddeningly difficult to find.

2 Case Study: Hacking a Presidential Election

The most sensational hacktivist attack took place during Ukraine's presidential elections. On 21 May 2014, CyberBerkut compromised the Central Election Commission (CEC), disabling core CEC network nodes and numerous components of the election system. For nearly 20 hours, the software, which was designed to display real-time updates in the vote count, did not work properly. On 25 May – election day – 12 minutes before the polls closed (19:48 EET), the attackers posted on the CEC website a picture of Ukrainian Right Sector leader Dmitry Yarosh, incorrectly claiming that he had won the election. This image was immediately shown on Russian TV channels.

It is important to note here that this attack could in no way have determined the outcome of the election. In Ukraine, every citizen inks his or her vote on a real paper

[3] For background on this hacker group, see Wikipedia entry 'CyberBerkut,' https://en.wikipedia.org/wiki/CyberBerkut.

ballot, and all votes are manually verified. Each polling station in every corner of the country physically delivers its ballots to CEC headquarters in Kyiv for aggregation, reconciliation, and determination of the final tally. CEC's information technology (IT) infrastructure is a complex, geographically distributed system designed for fault tolerance and transparency. Polling stations have an 'anti-fraud' design that allows monitors to detect anomalies such as dramatically swinging vote counts and report them to the appropriate authorities. Any serious disruption during an election would generate immediate suspicion about its legitimacy, and spark a desire for a new election.

That said, I believe that we should not underestimate the ability of hackers – especially those that enjoy state sponsorship – to disrupt the political process of a nation. If CEC's network had not been restored by 25 May, the country would simply have been unable to follow the vote count in real-time. However, to what extent would that have caused citizens to question the integrity of the entire process? It is hard to know.

CEC was not the only election-related site compromised. There were many others, including some that were only tangentially related to Ukrainian politics when, for example, the word 'election' had unfortunately appeared somewhere on the site. But even when attacks against low-level sites were unsophisticated, and the sites basically continued to function, the attackers still got the press attention they sought.

The technical aspects of this hack also tell us something very important: the hackers were professionals. Beyond disabling the site and successfully displaying incorrect election results, CERT-UA discovered advanced cyber espionage malware on the CEC network (Sofacy/APT28/Sednit). These two aspects of the attack – disruption and espionage – may seem contradictory, but in fact they are quite complementary. Hackers must first conduct in-depth reconnaissance of a target prior to any serious attack.

> *The technical aspects of this hack also tell us something very important: the hackers were professionals.*

To bolster its technical credentials as an elite hacker group, CyberBerkut claimed to have discovered and exploited a 'zero-day' vulnerability in CEC's Cisco ASA software. In my opinion, it is highly unlikely that a non-state hacker group would possess such a high level of technical expertise. If CyberBerkut really did exploit a zero-day, the group is likely supported by a nation-state.

During my tenure as chief of CERT-UA, the CEC compromise was probably the most technically advanced cyber attack we investigated. It was well planned, highly targeted, and had some (albeit limited) real-world impact. Preparation for such an attack does not happen overnight; based on our analysis of Internet Protocol (IP) activity, the attackers began their reconnaissance in mid-March 2014 – more than two months prior to the election. Neither does the level of required expertise suggest that this was the work of amateurs; at a minimum, the hackers had gained administrator-level access to CEC's network.

3 Conclusion: What Is to Be Done?

Ukraine today faces cyber security challenges on at least two fronts. First, there are technical attacks against a wide range of network infrastructure, including individual websites and whole Internet Service Providers (ISPs). These encompass everything from preoperational reconnaissance to social engineering against the target's employees. Second, there is an ongoing, content-driven information war within the online media space designed to influence and deceive the public.

More serious threats lie over the horizon. In recent incident response activities we have discovered samples of the most advanced forms of malware, including BlackEnergy2/SandWorm, Potao, Turla/Urobros, and more.

In the face of these threats, Ukraine is currently unprepared. At the strategic level, our senior officials are preoccupied with more pressing concerns. At the tactical level, our law enforcement agencies still fail to grasp the basic connection between email attachments, remote administrative software, and cyber espionage. Today, there is no unified mechanism to monitor Ukraine's network space, which hinders our ability to detect cases of unauthorised access in a timely fashion.

> *It is time for the government of Ukraine to pay attention to cyber security.*

It is time for the government of Ukraine to pay greater attention to cyber security. Given our current national security crisis, this will not be easy. However, in spite of the challenging environment, many positive developments are taking place in Ukraine, such as the recent transformation of Kyiv's metropolitan police force.[4] A similar breakthrough can take place in our cyber security domain, but it must begin with the allocation of funds to hire and retain the right personnel through competitive salaries and more attractive working conditions.

[4] Laura Mills. 'In Ukraine's Capital, a New Show of Force,' *The Wall Street Journal*, 6 August 2015, http://www.wsj.com/articles/in-ukraines-capital-a-new-show-of-force-1438903782.