The Hunt for Lurk

By Ruslan Stoyanov

Published: 2016-08-30 · Archived: 2026-04-05 13:25:18 UTC

In early June, 2016, the Russian police arrested the alleged members of the criminal group known as Lurk. The police suspected Lurk of stealing nearly three billion rubles, using malicious software to systematically withdraw large sums of money from the accounts of commercial organizations, including banks. For Kaspersky Lab, these arrests marked the culmination of a six-year investigation by the company's Computer Incidents Investigation team. We are pleased that the police authorities were able to put the wealth of information we accumulated to good use: to detain suspects and, most importantly, to put an end to the theft. We ourselves gained more knowledge from this investigation than from any other. This article is an attempt to share this experience with other experts, particularly the IT security specialists in companies and financial institutions that increasingly find themselves the targets of cyber-attacks.

When we first encountered Lurk, in 2011, it was a nameless Trojan. It all started when we became aware of a number of incidents at several Russian banks that had resulted in the theft of large sums of money from customers. To steal the money, the unknown criminals used a hidden malicious program that was able to interact automatically with the financial institution's remote banking service (RBS) software; replacing bank details in payment orders generated by an accountant at the attacked organization, or even generating such orders by itself.

In 2016, it is hard to imagine banking software that does not demand some form of additional authentication, but things were different back in 2011. In most cases, the attackers only had to infect the computer on which the RBS software was installed in order to start stealing the cash. Russia's banking system, like those of many other countries, was unprepared for such attacks, and cybercriminals were quick to exploit the security gap.

We participated in the investigation of several incidents involving the nameless malware, and sent samples to our malware analysts. They created a signature to see if any other infections involving it had been registered, and discovered something very unusual: our internal malware naming system insisted that what we were looking at was a Trojan that could be used for many things (spamming, for example) but not stealing money.

Our detection systems suggest that a program with a certain set of functions can sometimes be mistaken for something completely different. In the case of this particular program the cause was slightly different: an investigation revealed that it had been detected by a "common" signature because it was doing nothing that could lead the system to include it in any specific group, for example, that of banking Trojans.

Whatever the reason, the fact remained that the malicious program was used for the theft of money.

So we decided to take a closer look at the malware. The first attempts to understand how the program worked gave our analysts nothing. Regardless of whether it was launched on a virtual or a real machine, it behaved in the same way: it didn't do anything. This is how the program, and later the group behind it, got its name. To "lurk" means to hide, generally with the intention of ambush.

We were soon able to help investigate another incident involving Lurk. This time we got a chance to explore the image of the attacked computer. There, in addition to the familiar malicious program, we found a .dll file with which the main executable file could interact. This was our first piece of evidence that Lurk had a modular structure.

Later discoveries suggest that, in 2011, Lurk was still at an early stage of development. It was formed of just two components, a number that would grow considerably over the coming years.

The additional file we uncovered did little to clarify the nature of Lurk. It was clear that it was a Trojan targeting RBS and that it was used in a relatively small number of incidents. In 2011, attacks on such systems were starting to grow in popularity. Other, similar, programs were already known about, the earliest detected as far back as in 2006, with new malware appearing regularly since then. These included ZeuS, SpyEye, and Carberp, etc. In this series, Lurk represented yet another dangerous piece of malware.

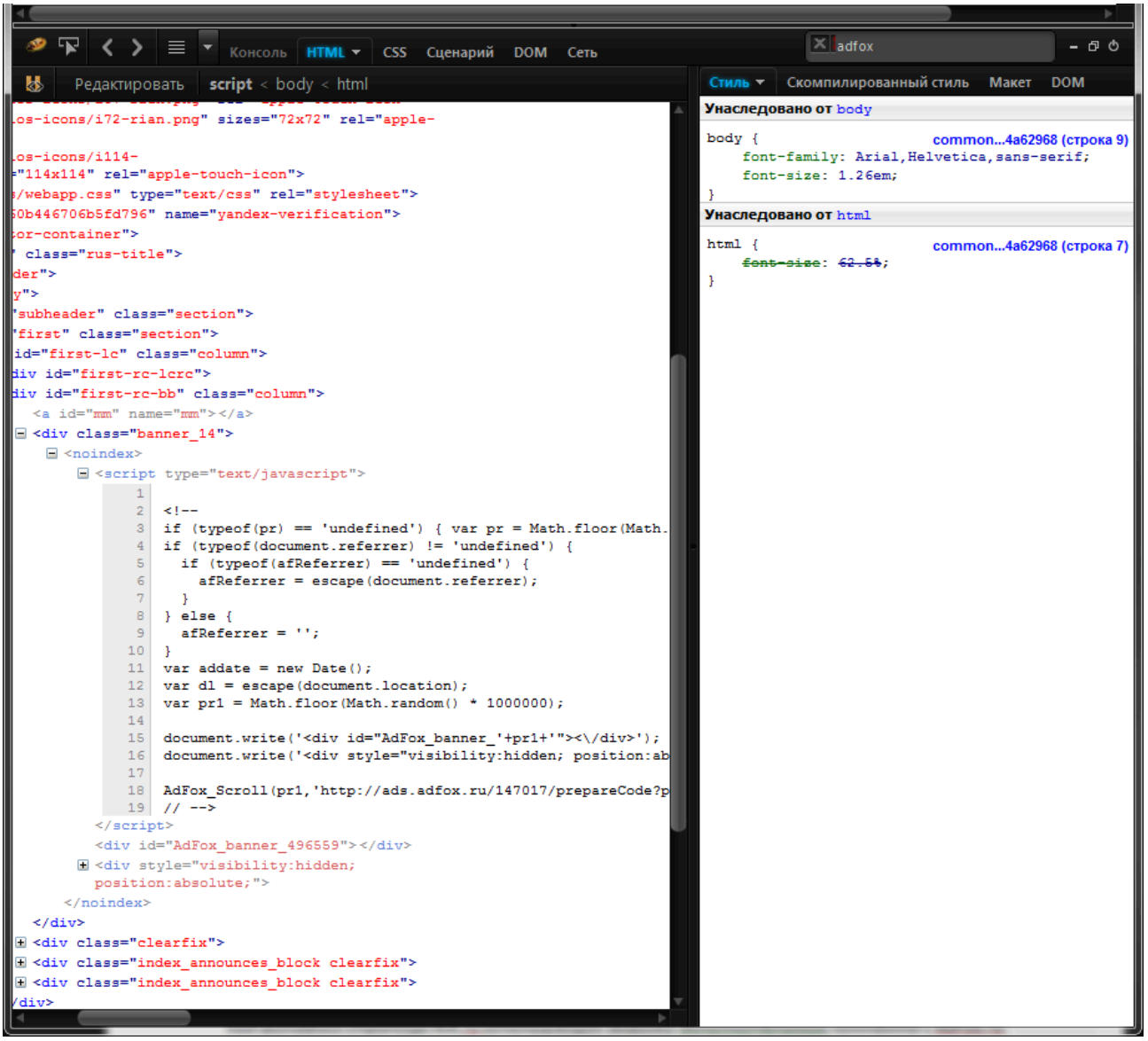
It was extremely difficult to make Lurk work in a lab environment. New versions of the program appeared only rarely, so we had few opportunities to investigate new incidents involving Lurk. A combination of these factors influenced our decision to postpone our active investigation into this program and turn our attention to more urgent tasks.

A change of leader

For about a year after we first met Lurk, we heard little about it. It later turned out that the incidents involving this malicious program were buried in the huge amount of similar incidents involving other malware. In May 2011, the source code of ZeuS had been published on the Web and this resulted in the emergence of many program modifications developed by small groups of cybercriminals.

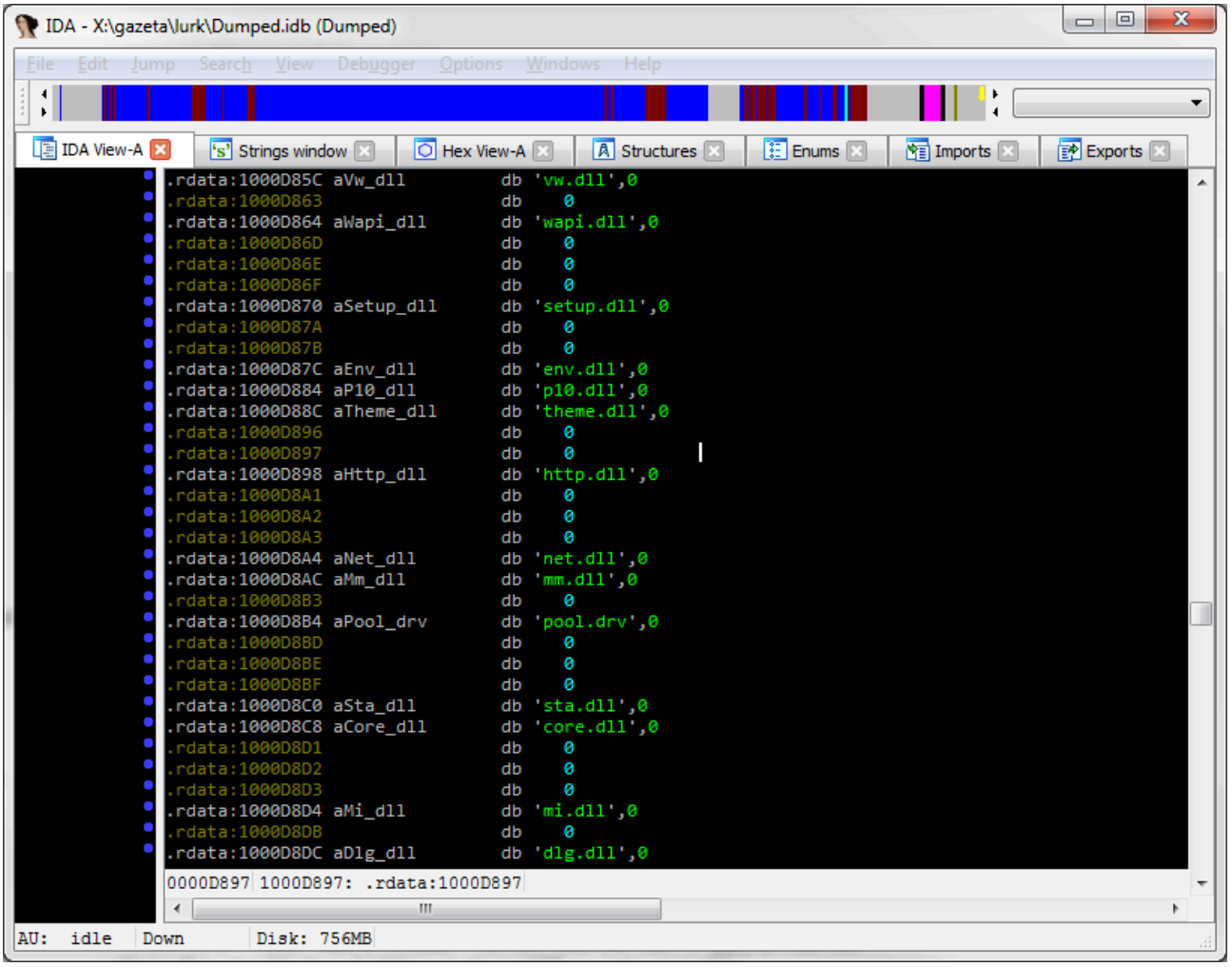
In addition to ZeuS, there were a number of other unique financial malware programs. In Russia, there were several relatively large cybercriminal groups engaged in financial theft via attacks on RBS. Carberp was the most active among them. At the end of March 2012, the majority of its members were arrested by the police. This event significantly affected the Russian cybercriminal world as the gang had stolen hundreds of millions of rubles during a few years of activity, and was considered a “leader” among cybercriminals. However, by the time of the arrests, Carberp’s reputation as a major player was already waning. There was a new challenger for the crown.

A few weeks before the arrests, the sites of a number of major Russian media, such as the agency “RIA Novosti”, Gazeta.ru and others, had been subjected to a watering hole attack. The unknown cybercriminals behind this attack distributed their malware by exploiting a vulnerability in the websites’ banner exchange system. A visitor to the site would be redirected to a fraudulent page containing a Java exploit. Successful exploitation of the vulnerability initiated the launch of a malicious program whose main function was collecting information on the attacked computer, sending it to a malicious server, and in some cases receiving and installing an extra load from the server.



The code on the main page of RIA.ru that is used to download additional content from AdFox.ru

From a technical perspective, the malicious program was unusual. Unlike most other malware, it left no traces on the hard drive of the system attacked and worked only in the RAM of the machine. This approach is not often used in malware, primarily because the resulting infection is “short-lived”: malware exists in the system only until the computer is restarted, at which point the process of infection need to be started anew. But, in the case of these attacks, the secret “bodiless” malicious program did not have to gain a foothold in the victim’s system. Its primary job was to explore; its secondary role was to download and install additional malware. Another fascinating detail was the fact that the malware was only downloaded in a small number of cases, when the victim computer turned out to be “interesting”.



Part of the Lurk code responsible for downloading additional modules

Analysis of the bodiless malicious program showed that it was “interested” in computers with remote banking software installed. More specifically, RBS software created by Russian developers. Much later we learned that this unnamed, bodiless module was a mini, one of the malicious programs which used Lurk. But at the time we were not sure whether the Lurk we had known since 2011, and the Lurk discovered in 2012, were created by the same people. We had two hypotheses: either Lurk was a program written for sale, and both the 2011 and 2012 versions were the result of the activity of two different groups, which had each bought the program from the author; or the 2012 version was a modification of the previously known Trojan.

The second hypothesis turned out to be correct.

Invisible war with banking software

A small digression. Remote banking systems consist of two main parts: the bank and the client. The client part is a small program that allows the user (usually an accountant) to remotely manage their organization’s accounts. There are only a few developers of such software in Russia, so any Russian organization that uses RBS relies on software developed by one of these companies. For cybercriminal groups specializing in attacks on RBS, this limited range of options plays straight into their hands.

In April 2013, a year after we found the “bodiless” Lurk module, the Russian cybercriminal underground exploited several families of malicious software that specialized in attacks on banking software. Almost all operated in a similar way: during the exploration stage they found out whether the attacked computer had the necessary banking software installed. If it did, the malware downloaded additional modules, including ones allowing for the automatic creation of unauthorized payment orders, changing details in legal payment orders, etc. This level of automation became possible because the cybercriminals had thoroughly studied how the banking software operated and “tailored” their malicious software modules to a specific banking solution.

The people behind the creation and distribution of Lurk had done exactly the same: studying the client component of the banking software and modifying their malware accordingly. In fact, they created an illegal add-on to the legal RBS product.

Through the information exchanges used by people in the security industry, we learned that several Russian banks were struggling with malicious programs created specifically to attack a particular type of legal banking software. Some of them were having to release weekly patches to customers. These updates would fix the immediate security problems, but the mysterious hackers “on the other side” would quickly release a new version of malware that bypassed the upgraded protection created by the authors of the banking programs.

It should be understood that this type of work – reverse-engineering a professional banking product – cannot easily be undertaken by an amateur hacker. In addition, the task is tedious and time-consuming and not the kind to be performed with great enthusiasm. It would need a team of specialists. But who in their right mind would openly take up illegal work, and who might have the money to finance such activities? In trying to answer these questions, we eventually came to the conclusion that every version of Lurk probably had an organized group of cybersecurity specialists behind it.

The relative lull of 2011-2012 was followed by a steady increase in notifications of Lurk-based incidents resulting in the theft of money. Due to the fact that affected organizations turned to us for help, we were able to collect ever more information about the malware. By the end of 2013, the information obtained from studying hard drive images of attacked computers as well as data available from public sources, enabled us to build a rough picture of a group of Internet users who appeared to be associated with Lurk.

This was not an easy task. The people behind Lurk were pretty good at anonymizing their activity on the network. For example, they were actively using encryption in everyday communication, as well as false data for domain registration, services for anonymous registration, etc. In other words, it was not as easy as simply looking someone up on “Vkontakte” or Facebook using the name from Whois, which can happen with other, less professional groups of cybercriminals, such as Koobface. The Lurk gang did not make such blunders. Yet mistakes, seemingly insignificant and rare, still occurred. And when they did, we caught them.

Not wishing to give away free lessons in how to run a conspiracy, I will not provide examples of these mistakes, but their analysis allowed us to build a pretty clear picture of the key characteristics of the gang. We realized that we were dealing with a group of about 15 people (although by the time it was shut down, the number of “regular” members had risen to 40). This team provided the so-called “full cycle” of malware development, delivery and monetization – rather like a small, software development company. At that time the “company” had two key “products”: the malicious program, Lurk, and a huge botnet of computers infected with it. The malicious program

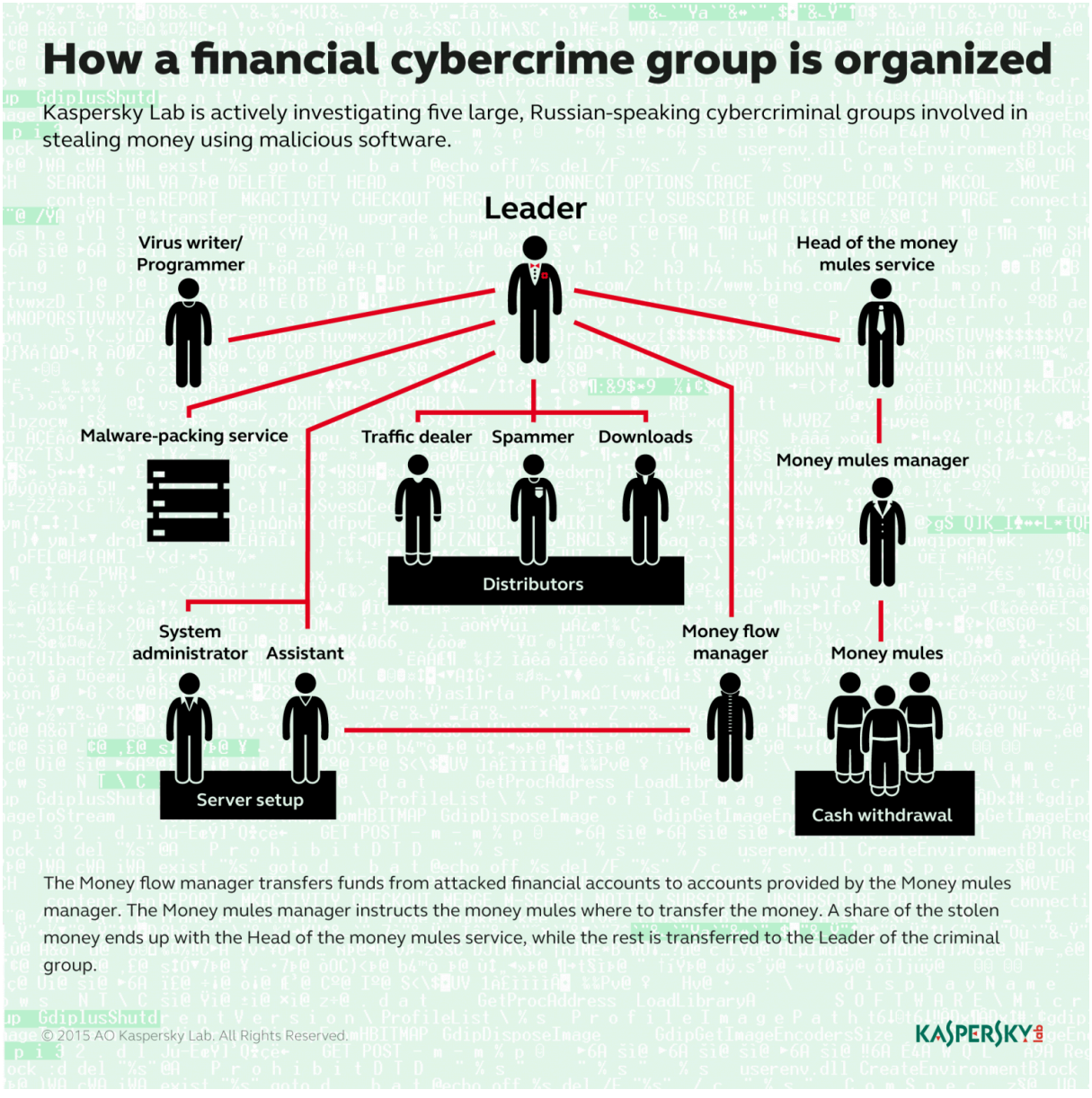
had its own team of developers, responsible for developing new functions, searching for ways to “interact” with RBS systems, providing stable performance and fulfilling other tasks. They were supported by a team of testers who checked the program performance in different environments. The botnet also had its own team (administrators, operators, money flow manager, and other partners working with the bots via the administration panel) who ensured the operation of the command and control (C&C) servers and protected them from detection and interception.

Developing and maintaining this class of malicious software requires professionals and the leaders of the group hunted for them on job search sites. Examples of such vacancies are covered in my article about Russian financial cybercrime. The description of the vacancy did not mention the illegality of the work on offer. At the interview, the “employer” would question candidates about their moral principles: applicants were told what kind of work they would be expected to do, and why. Those who agreed got in.

A fraudster has advertised a job vacancy for java / flash specialists on a popular Ukrainian website. The job requirements include a good level of programming skills in Java, Flash, knowledge of JVM / AVM specifications, and others. The organizer offers remote work and full employment with a salary of $2,500.

So, every morning, from Monday to Friday, people in different parts of Russia and Ukraine sat down in front of their computer and started to “work”. The programmers “tuned” the functions of malware modifications, after which the testers carried out the necessary tests on the quality of the new product. Then the team responsible for the botnet and for the operation of the malware modules and components uploaded the new version onto the command server, and the malicious software on botnet computers was automatically updated. They also studied information sent from infected computers to find out whether they had access to RBS, how much money was deposited in clients’ accounts, etc.

The money flow manager, responsible for transferring the stolen money into the accounts of money mules, would press the button on the botnet control panel and send hundreds of thousands of rubles to accounts that the “drop project” managers had prepared in advance. In many cases they didn’t even need to press the button: the malicious program substituted the details of the payment order generated by the accountant, and the money went directly to the accounts of the cybercriminals and on to the bank cards of the money mules, who cashed it via ATMs, handed it over to the money mule manager who, in turn, delivered it to the head of the organization. The head would then allocate the money according to the needs of the organization: paying a “salary” to the employees and a share to associates, funding the maintenance of the expensive network infrastructure, and of course, satisfying their own needs. This cycle was repeated several times.



Each member of the typical criminal group has their own responsibilities.

These were the golden years for Lurk. The shortcomings in RBS transaction protection meant that stealing money from a victim organization through an accountant’s infected machine did not require any special skills and could even be automated. But all “good things” must come to an end.

The end of “auto money flow” and the beginning of hard times

The explosive growth of thefts committed by Lurk and other cybercriminal groups forced banks, their IT security teams and banking software developers to respond.

First of all, the developers of RBS software blocked public access to their products. Before the appearance of financial cybercriminal gangs, any user could download a demo version of the program from the manufacturer’s website. Attackers used this to study the features of banking software in order to create ever more tailored malicious programs for it. Finally, after many months of “invisible war” with cybercriminals, the majority of RBS software vendors succeeded in perfecting the security of their products.

At the same time, the banks started to implement dedicated technologies to counter the so-called “auto money flow”, the procedure which allowed the attackers to use malware to modify the payment order and steal money automatically.

By the end of 2013, we had thoroughly explored the activity of Lurk and collected considerable information about the malware. At our farm of bots, we could finally launch a consistently functioning malicious script, which allowed us to learn about all the modifications cybercriminals had introduced into the latest versions of the program. Our team of analysts had also made progress: by the year’s end we had a clear insight into how the malware worked, what it comprised and what optional modules it had in its arsenal.

Most of this information came from the analysis of incidents caused by Lurk-based attacks. We were simultaneously providing technical consultancy to the law enforcement agencies investigating the activities of this gang.

It was clear that the cybercriminals were trying to counteract the changes introduced in banking and IT security. For example, once the banking software vendors stopped providing demo versions of their programs for public access, the members of the criminal group established a shell company to receive directly any updated versions of the RBS software.

Thefts declined as a result of improvements in the security of banking software, and the “auto money flow” became less effective. As far as we can judge from the data we have, in 2014 the criminal group behind Lurk seriously reduced its activity and “lived from hand to mouth”, attacking anyone they could, including ordinary users. Even if the attack could bring in no more than a few tens of thousands of rubles, they would still descend to it.

In our opinion, this was caused by economic factors: by that time, the criminal group had an extensive and extremely costly network infrastructure, so, in addition to employees’ salaries, it was necessary to pay for renting servers, VPN and other technical tools. Our estimates suggest that the network infrastructure alone cost the Lurk managers tens of thousands of dollars per month.

Attempts to come back

In addition to increasing the number of “minor” attacks, the cybercriminals were trying to solve their cash flow problem by “diversifying” the business and expanding their field of activity. This included developing,

maintaining and renting the Angler exploit pack (also known as XXX). Initially, this was used mainly to deliver Lurk to victims' computers. But as the number of successful attacks started to decline, the owners began to offer smaller groups paid access to the tools.

By the way, judging by what we saw on Russian underground forums for cybercriminals, the Lurk gang had an almost legendary status. Even though many small and medium-sized groups were willing to "work" with them, they always preferred to work by themselves. So when Lurk provided other cybercriminals with access to Angler, the exploit pack became especially popular – a "product" from the top underground authority did not need advertising. In addition, the exploit pack was actually very effective, delivering a very high percentage of successful vulnerability exploitations. It didn't take long for it to become one of the key tools on the criminal2criminal market.

As for extending the field of activity, the Lurk gang decided to focus on the customers of major Russian banks and the banks themselves, whereas previously they had chosen smaller targets.

In the second half of 2014, we spotted familiar pseudonyms of Internet users on underground forums inviting specialists to cooperate on document fraud. Early the following year, several Russian cities were swamped with announcements about fraudsters who used fake letters of attorney to re-issue SIM cards without their owners being aware of it.

The purpose of this activity was to gain access to one-time passwords sent by the bank to the user so that they could confirm their financial transaction in the online or remote banking system. The attackers exploited the fact that, in remote areas, mobile operators did not always carefully check the authenticity of the documents submitted and released new SIM cards at the request of cybercriminals. Lurk would infect a computer, collect its owner's personal data, generate a fake letter of attorney with the help of "partners" from forums and then request a new SIM card from the network operator.

Once the cybercriminals received a new SIM card, they immediately withdrew all the money from the victim's account and disappeared.

Although initially this scheme yielded good returns, this didn't last long, since by then many banks had already implemented protection mechanisms to track changes in the unique SIM card number. In addition, the SIM card-based campaign forced some members of the group and their partners out into the open and this helped law enforcement agencies to find and identify suspects.

Alongside the attempts to "diversify" the business and find new cracks in the defenses of financial businesses, Lurk continued to regularly perform "minor thefts" using the proven method of auto money flow. However, the cybercriminals were already planning to earn their main money elsewise.

New "specialists"

In February 2015, Kaspersky Lab's Global Research and Analysis Team (GReAT) released its research into the Carbanak campaign targeting financial institutions. Carbanak's key feature, which distinguished it from "classical" financial cybercriminals, was the participation of professionals in the Carbanak team, providing deep knowledge of the target bank's IT infrastructure, its daily routine and the employees who had access to the

software used to conduct financial transactions. Before any attack, Carbanak carefully studied the target, searched for weak points and then, at a certain moment in time, committed the theft in no more than a few hours. As it turned out, Carbanak was not the only group applying this method of attack. In 2015, the Lurk team hired similar experts.

How the Carbanak group operated.

We realized this when we found incidents that resembled Carbanak in style, but did not use any of its tools. This was Lurk. The Lurk malware was used as a reliable “back door” to the infrastructure of the attacked organization rather than as a tool to steal money. Although the functionality that had previously allowed for the near-automatic theft of millions no longer worked, in terms of its secrecy Lurk was still an extremely dangerous and professionally developed piece of malware.

However, despite its attempts to develop new types of attacks, Lurk’s days were numbered. Thefts continued until the spring of 2016. But, either because of an unshakable confidence in their own impunity or because of apathy, day-by-day the cybercriminals were paying less attention to the anonymity of their actions. They became especially careless when cashing money: according to our incident analysis, during the last stage of their activity, the cybercriminals used just a few shell companies to deposit the stolen money. But none of that mattered any more as both we and the police had collected enough material to arrest suspected group members, which happened early in June this year.

No one on the Internet knows you are a cybercriminal?

My personal experience of the Lurk investigation made me think that the members of this group were convinced they would never be caught. They had grounds to be that presumptuous: they were very thorough in concealing the traces of their illegal activity, and generally tried to plan the details of their actions with care. However, like all

people, they made mistakes. These errors accumulated over the years and eventually made it possible to put a stop to their activity. In other words, although it is easier to hide evidence on the Internet, some traces cannot be hidden, and eventually a professional team of investigators will find a way to read and understand them.

Lurk is neither the first nor the last example to prove this. The infamous banking Trojan SpyEye was used to steal money between 2009 and 2011. Its alleged creator was arrested 2013, and convicted in 2014.

The first attacks involving the banking Trojan Carberp began in 2010; the members of the group suspected of creating and distributing this Trojan were arrested in 2012 and convicted in 2014. The list goes on.

The history of these and other cybercriminal groups spans the time when everyone (and members of the groups in particular) believed that they were invulnerable and the police could do nothing. The results have proved them wrong.

Unfortunately, Lurk is not the last group of cybercriminals attacking companies for financial gain. We know about some other groups targeting organizations in Russia and abroad. For these reasons, we recommend that all organizations do the following:

- If your organization was attacked by hackers, immediately call the police and involve experts in digital forensics. The earlier you apply to the police, the more evidence the forensics will able to collect, and the more information the law enforcement officers will have to catch the criminals.
- Apply strict IT security policies on terminals from which financial transactions are made and for employees working with them.
- Teach all employees who have access to the corporate network the rules of safe online behavior.

Compliance with these rules will not completely eliminate the risk of financial attacks but will make it harder for fraudsters and significantly increase the probability of their making a mistake while trying to overcome these difficulties. And this will help law enforcement agencies and IT security experts in their work.

P.S.: why does it take so long?

Law enforcement agencies and IT security experts are often accused of inactivity, allowing hackers to remain at large and evade punishment despite the enormous damage caused to the victims.

The story of Lurk proves the opposite. In addition, it gives some idea of the amount of work that has to be done to obtain enough evidence to arrest and prosecute suspects. Unfortunately, the rules of the “game” are not the same for all participants: the Lurk group used a professional approach to organizing a cybercriminal enterprise, but, for obvious reasons, did not find it necessary to abide by the law. As we work with law enforcement, we must respect the law. This can be a long process, primarily because of the large number of “paper” procedures and restrictions that the law imposes on the types of information we as a commercial organization can work with.

Our cooperation with law enforcement in investigating the activity of this group can be described as a multi-stage data exchange. We provided the intermediate results of our work to the police officers; they studied them to understand if the results of our investigation matched the results of their research. Then we got back our data “enriched” with the information from the law enforcement agencies. Of course, it was not all the information they

could find; but it was the part which, by law, we had the right to work with. This process was repeated many times until we finally we got a complete picture of Lurk activity. However, that was not the end of the case.

A large part of our work with law enforcement agencies was devoted to “translating” the information we could get from “technical” into “legal” language. This ensured that the results of our investigation could be described in such a way that they were clear to the judge. This is a complicated and laborious process, but it is the only way to bring to justice the perpetrators of cybercrimes.

Source: https://securelist.com/the-hunt-for-lurk/75944/