Secrets of Cobalt

Archived: 2026-05-01 02:01:41 UTC

In June 2016, **the first attack conducted by the Cobalt group was tracked at a large Russian bank**, where hackers attempted to steal money from ATMs. The attackers infiltrated the bank's network, gained control over it, compromised the domain administrator's account, and reached the ATM control server.

The Bank's Information Security team detected traces of malicious programs and suspicious connections to the server. In order to stop further unauthorized access, the entire bank was blocked from accessing the Internet. This turned out to be the best solution, as the Cobalt group set up a controlled botnet in the bank's network which was very difficult to track and even harder to stop.

The day after the attack, Group-IB experts came to the bank's central office and began searching for the source of the attack; ascertaining the stages of its development, causes, and consequences; analyzing the malicious programs; and restoring the chain of events. The computers that were involved in the attack were then examined.

Group-IB forensic specialists immediately understood that they faced a new approach to targeted attacks on banks. They were not wrong. The June incident was a "test" of a new attack technique that the attackers would begin using in July in the CIS, Europe, and Asia. For example, **over $2m USD was stolen from 34 ATMs** operated by the First Bank, one of Taiwan's largest banks. In october 2016 Group-IB published the report about the Cobalt group. Now, a year later, this group is continuing to attack banks, which is reported monthly by Group-IB's Threat Intelligence team.

Initially the Cobalt group focused on jackpotting ATMs: they launched a program that sent commands directly to the dispenser to issue cash. Then the group shifted to other systems in the bank including card processing, payment systems, SWIFT. Once gaining access to such systems, attackers studied how payments and other financial transactions are conducted to repeat them. That said, the services, such as payment processing systems or SWIFT are not actually hacked or the 'weak point'. The actual vulnerability is the bank and the protection methods against such advanced attacks.

The Cobalt group's attacks are always executed according to the same template. The basic principles of targeted attacks on financial institutions have not changed since 2013 when the Anunak, Corkow, Buhtrap, and Lurk groups began conducting the first attacks on Russian banks. The only thing that has changed is the tools. Attack stages are shown in *fig. 1.*

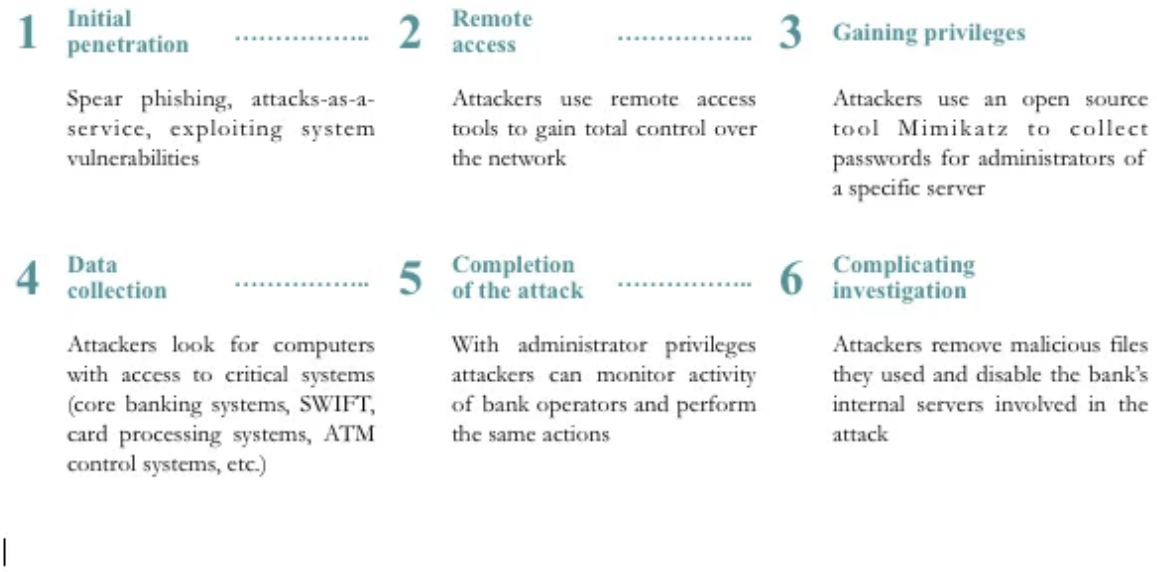
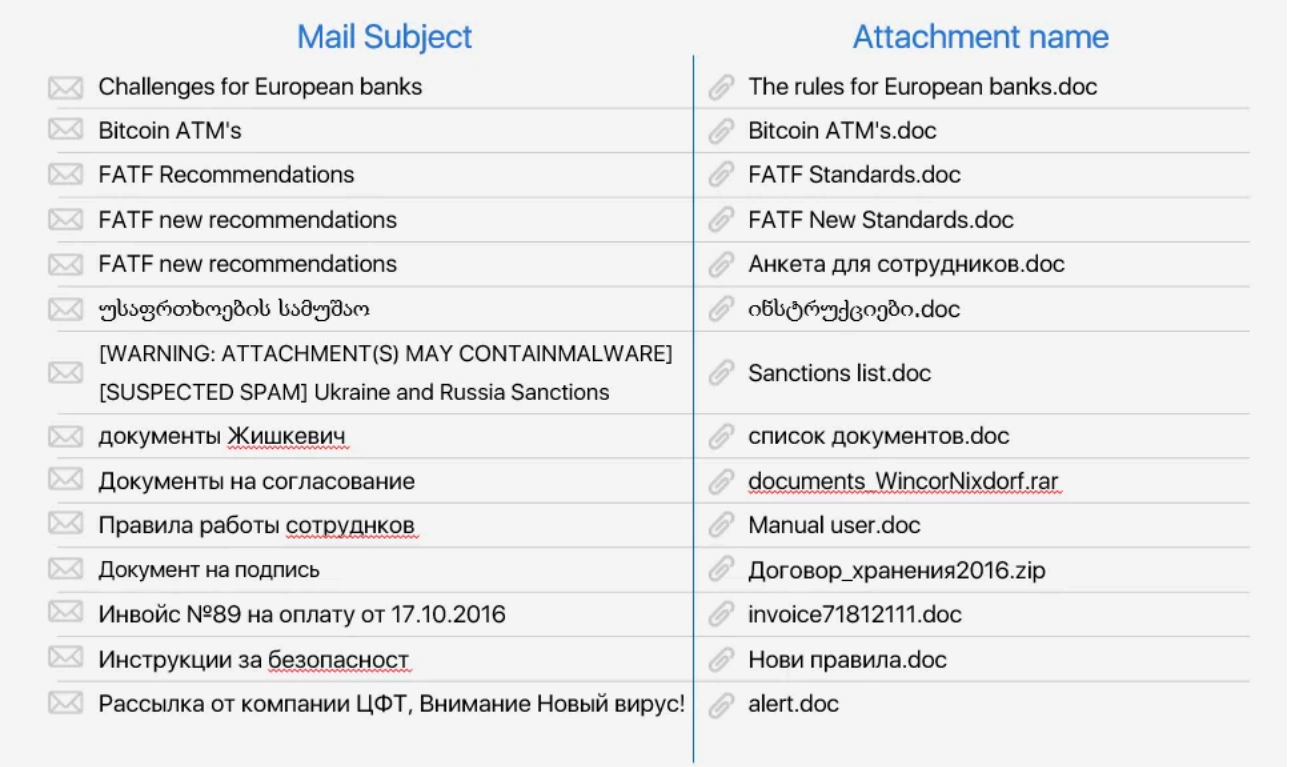


Fig. 1 The Cobalt group's stages of attack

Currently, the Cobalt group is attacking large financial organizations around the world, that's why it makes sense to talk about the techniques used by this group to conceal their traces in the network and circumvent security measures.

Network penetration

In all cases investigated by Group-IB, **the Cobalt group used a set of spear phishing emails to gain initial access to the corporate infrastructure**. The attackers use mail servers to carry out mass mailing of phishing messages containing attachments to employees of the organization of interest. Message subjects and attachment names are written in such a way that the employees want to open them *(fig. 2)*.



Mail Subject	Attachment name
Challenges for European banks	The rules for European banks.doc
Bitcoin ATM's	Bitcoin ATM's.doc
FATF Recommendations	FATF Standards.doc
FATF new recommendations	FATF New Standards.doc
FATF new recommendations	Анкета для сотрудников.doc
უსაფრთხოების სამუშაო	ინსტრუქციები.doc
[WARNING: ATTACHMENT(S) MAY CONTAINMALWARE] [SUSPECTED SPAM] Ukraine and Russia Sanctions	Sanctions list.doc
документы Жишкевич	список документов.doc
Документы на согласование	documents_WincorNixdorf.rar
Правила работы сотрудников	Manual user.doc
Документ на подпись	Договор_хранения2016.zip
Инвойс №89 на оплату от 17.10.2016	invoice71812111.doc
Инструкции за безопасност	Нови правила.doc
Рассылка от компании ЦФТ, Внимание Новый вирус!	alert.doc

Fig. 2 Examples of message subjects and attachment names

The mailing is carried out on a mass scale: in any organization, messages are usually sent to between 10 and 40 employees. However, some of the email addresses belong to employees that no longer work at the organization, which means that the Cobalt group likely uses out-of-date mailing lists. Each message contains an attachment that loads the payload – part of Cobalt Strike software – to the computer's operating memory.

In order to make this download possible, **attackers have tried several different formats of attachments and emails, as their primary task is to bypass mail filters, protection measures, and the company's security policy.** First archives with .exe and .scr executables were used as an attachment *(fig. 3)*.

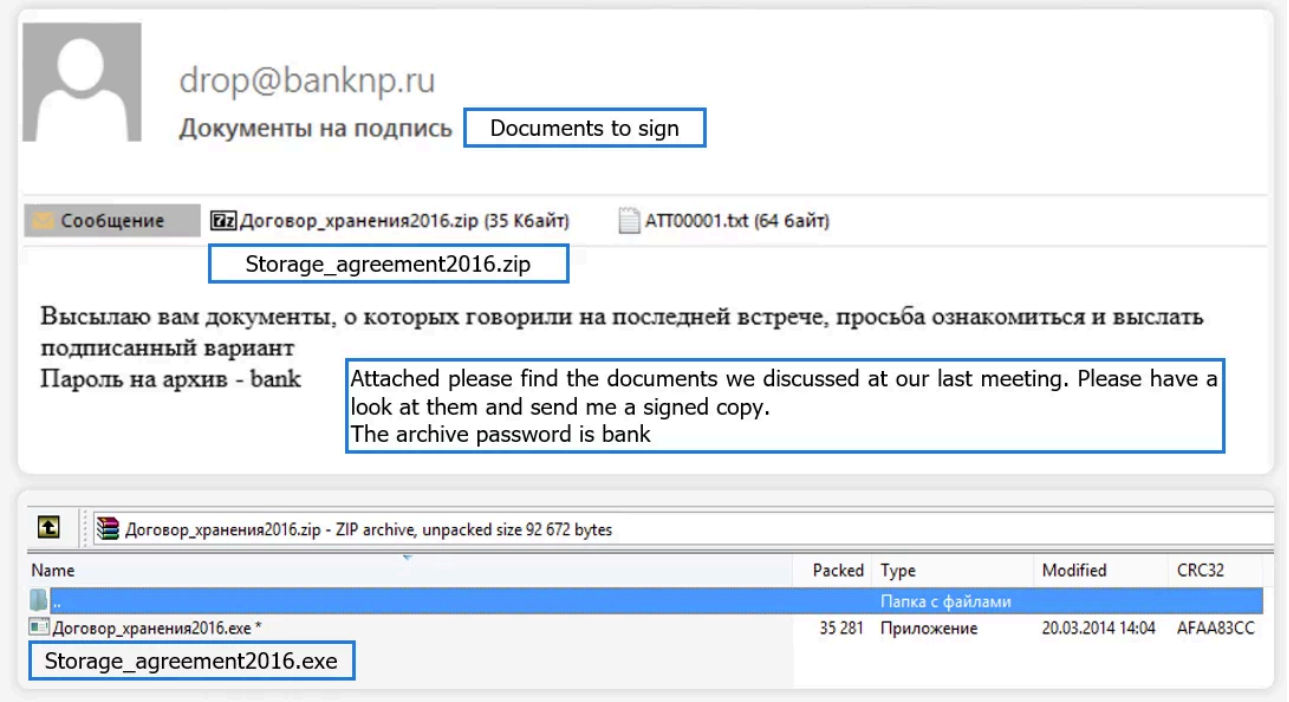


Fig. 3 Example of a message with an executable attachment (.exe)

The archive is password-protected in order to bypass anti-virus scans, security systems, and mail filters. However, when there is use of a security policy that prohibits the transfer of encrypted archives, such an email message may be blocked, so the attackers would send .doc files that contain exploits for Microsoft Office *(fig. 4)*.

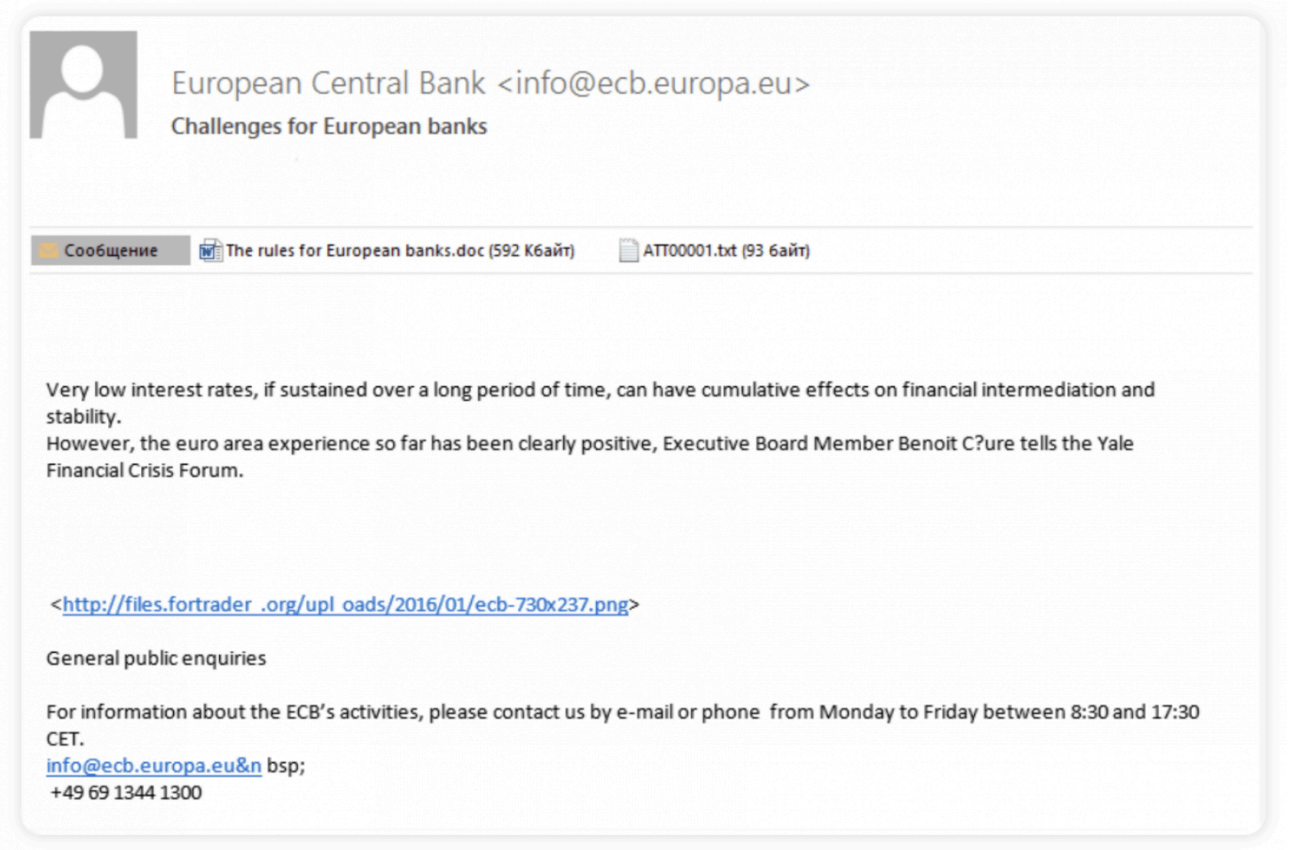


Fig. 4 The attackers would send .doc files that contain exploits for Microsoft Office.

This scheme assumes the presence of a vulnerable version of software. Companies can protect themselves by updating all software they use in a timely fashion. Of course, the risk of zero-day vulnerabilities remains, but we have not yet seen their use in these types of attacks. **For organizations that perform timely updates of their systems and adhere to strict security policies, the Cobalt group employs another method to deliver malicious code** through emails with Word documents containing a malicious macro. When opening the document, the user must click on the “Enable content” button, which enables macros *(fig. 5)*.

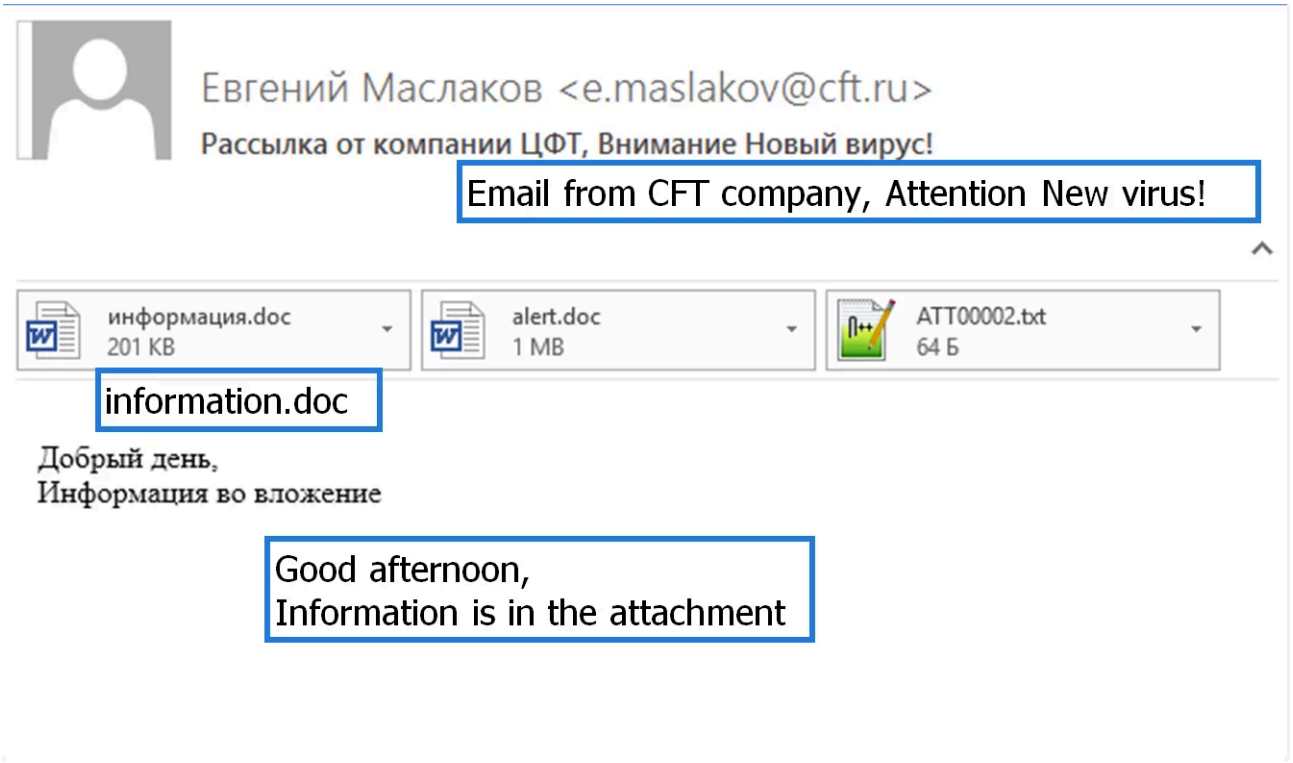


Fig. 5 Example of an email message with a Word document, which, when opened, requires the user to click on the “Enable content” button to enable a malicious macro.

One of Cobalt’s tasks when crafting spear-phishing emails is to conceal the sender. In events where of a simple substitution of the sender’s field, the majority of mail servers block these messages. Therefore, the Cobalt group registered domains are similar to real ones (for example, *diebold.pw*), and configured their email server to distribute acting as these legitimate domains *(fig. 6)*.

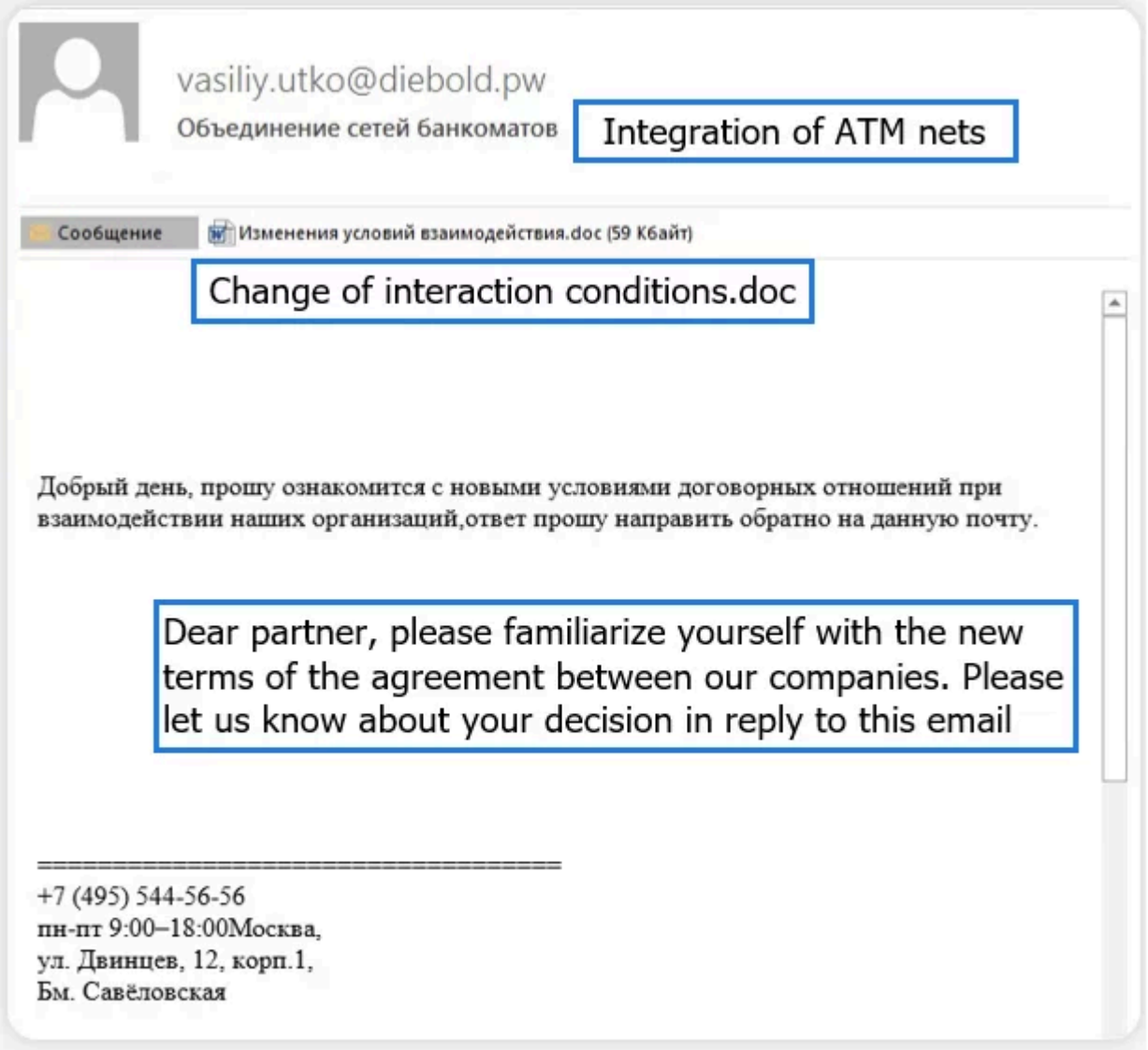


Fig. 6 Example of a message sent by attackers from a domain whose name is similar to the name of a real domain.

As soon as the attachment is launched and the malicious code is executed, the Cobalt Strike payload is loaded in the memory. This tool is used for penetration testing, which means that it isn't available only to cyber-fraudsters. This software provides a full set of functions for managing a downloaded module, and accordingly, an infected computer. This set includes a keylogger, screenshots, remote access via VNC, injections into processes, the ability to bypass the UAC security system, the Mimikatz tool, which is used to compromise access credentials for Windows OS accounts, the ability to scan open ports on an organization's computers, etc.

Running in RAM

Cobalt Strike modules aren't stored in the file system; their executable code can only be found in RAM. By default, the code runs in the context of rundll32.exe process, but can be injected into any process, for example, to increase the rights and number of privileges. In addition, Cobalt Strike enables users not to expose a fragment of memory allocated in the context of another process, the RWX (Read, Write, Execute) attributes, which often reveal injected code. Finally, not all anti-virus tools can scan RAM.

Provision of the malware survivability

The Cobalt group uses different methods to ensure malware survivability on corporate networks. The goal is to set the startup path to the executable file or program code, launching it with the powershell.exe shell command to access the Internet resource specified in the code in order to download and install Cobalt Strike module. In this way, the payload itself is not saved in the system, but rather is reloaded each time. Another bonus of this method is that a different payload can be loaded each time.

Startup is ensured only on several machines that have access to the Internet. As a response, the following startup methods have been recorded: through a service, startup registry keys, and Windows OS tasks, by replacing the legitimate executable software files prescribed in startup with the executable file of the attackers. From our experience, **the Cobalt group uses a new method to provide its survivability in every attack**. The danger of OS tasks is that their startup can be delayed. Even if the network is not infected now, in a month the corresponding task may work, and the payload will get into the organization's computers.

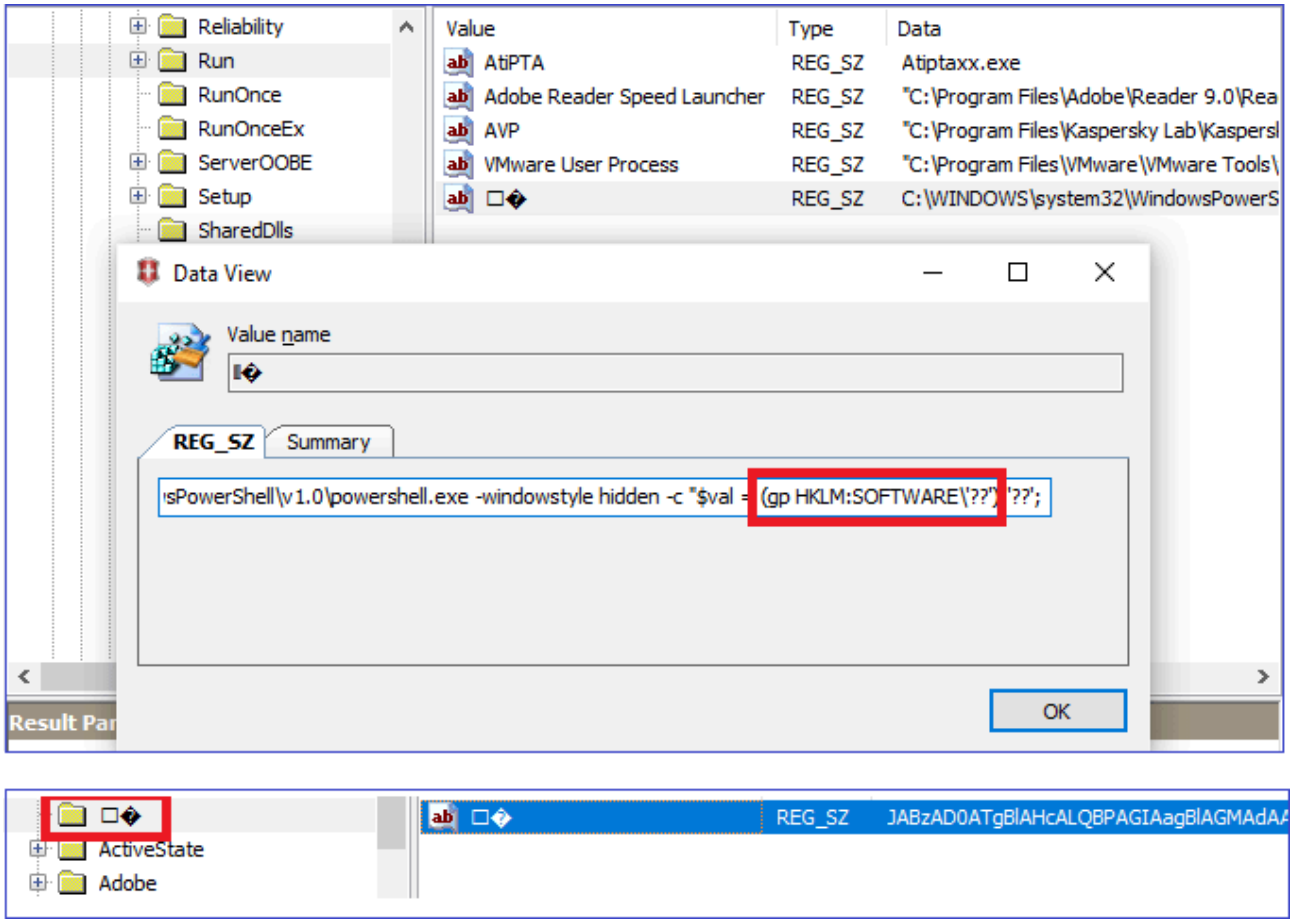


Fig. 7 Registry keys for startup

Bypassing anti-virus tools

Usually in spear-phishing emails, no exploits or any executable modules are detected by anti-virus tools (this has been the case with all active groups). The attackers try to reassemble the loaded modules in order to bypass the signature analysis of anti-virus tools. Cobalt Strike provides the ability to use the Artifact Kit framework for

these purposes and even modify it, as it is distributed in the source code. Aside from that, startup is performed by loading Cobalt Strike into the main memory without saving to the file system. Additional means of circumventing anti-virus tools include the use of exploits to increase the level of rights and privileges, bypassing UAC, and injecting code into trusted processes.

Bypassing network security

Cobalt Strike allows users to install two types of modules: HTTP/HTTPS/DNS modules and SMB modules. The former module is installed on a system that has access to the Internet and provides interaction with the C&C server using HTTP/HTTPS/DNS protocols. After the email message sent by the attackers is opened, such a module is downloaded to the system. Another module is installed even in systems that do not have Internet access, as, using SMB protocol (which is typically used within a local network), the SMB module is controlled via infected computers running the HTTP/HTTPS/DNS module.

To circumvent intrusion detection and prevention systems, as well as firewalls and proxy servers with signature rules aimed at detecting requests of a certain type, the Cobalt Strike modules generate communication profiles using the HTTP protocol: the value of the protocol's service header and query parameters are given, the data can be forwarded as header value, as the value of the parameter sent with the URI, as part of the URI, and sent in the body of HTTP message. When interacting with the C&C server, the data (executable files, commands, and the outputs of those commands) is encrypted. For interaction on HTTPS protocol, HTTP protocol profiles may be used with an indicated SSL certificate, but for data exchange on the DNS protocol, it requires DNS A, AAAA, and TXT records. In this case, one may separately specify the interaction intervals between the C&C server and the module on the infected computer.

The Cobalt Strike module can use several profiles and switch between data exchange methods on command from the C&C server without the need to update the module. The addresses of the C&C servers change from the moment the intruders penetrate the company's network until the moment the money is stolen, thus avoiding blacklists of IP addresses or domain names. In this way, a controlled botnet is created within the organization that has access to any computer, even those that do not have access to the Internet.

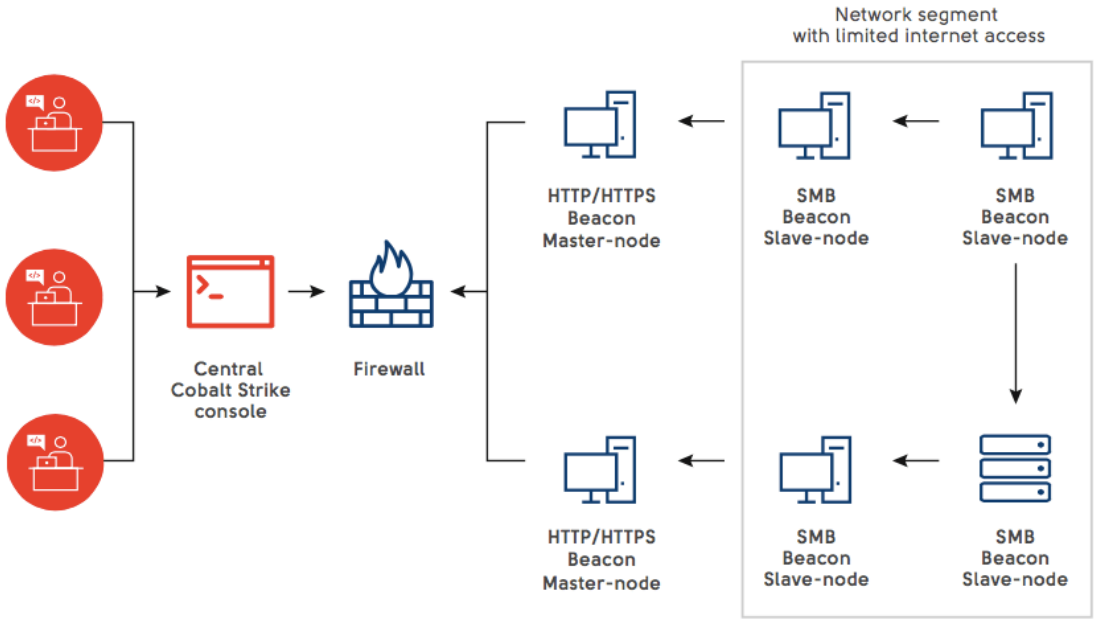


Fig.8 Cobalt Strike infrastructure

Network distribution

To run malicious programs on other computers on the network, including Cobalt Strike modules, the following methods are used, which are provided by Microsoft products for admin accounts to:

- Create a service on another computer to run the program code, start the service, and delete it. As for the command line, a program code is written and passed to the input of the powershell.exe command interpreter;
- Connect to a shared directory (C$, ADMIN$) on another computer, copy the module to it, create the service, run it to start the module, and then delete the service; delete the module.
- Connect to another computer using PsExec.exe (the remote access program is included in the Microsoft SysInternals suite), copy the module, and run it; delete the module.
- Connect to another computer via RDP, copy the module, and run it; delete the module.

After creation, the services are deleted. Remote access via RDP and using PsExec is typical for network administrators. Therefore, traces of programs that operate only in RAM are difficult to detect in a timely manner. Usually OS logs and memory dump can help. More detailed information can be obtained during an advanced security audit and by periodically making backup copies of these logs.

Use of standard tools

Cobalt Strike is publicly accessible, and can be downloaded in order to learn and create detection rules on the network. Aside from that, to work within an organization, the Cobalt group uses standard tools, including:

- remote connection via the RDP protocol (built-in capability of the OS);
- remote connection using PsExec;
- remote connection using TeamViewer, which allows a user to preserve remote access in case control using the Cobalt Strike module is lost;
- network scanning using the SoftPerfect Network Scanner program;
- secure connection using the Plink program.

To prevent this threat, the company should configure filter rules to detect the above-mentioned tools on the corporate network. TeamViewer calls can be controlled by rules on the firewall, proxy server, etc.

Conclusion

After infecting one computer on an organization's network, the Cobalt group analyzes the programs used on it and search for critical servers and the computers from which they are accessed. Financial organizations usually spend a lot of money on information security and consider their isolated subnets to be safe. However, all of these subnets are controlled by people, and there is practically always access to a secure subnet from an unsecured one, even if it's just from one computer with a unique account. This is exactly what attackers will be looking for. As we know from our experience, it takes from 2 weeks to 1.5 months to gain access to critical infrastructure.

This means that bank's information security specialists have, on average, one month to identify attackers on a network. Anti-virus solutions do not help, the only thing that can protect your company is knowledge of how, who, and with what tools hackers are attacking. That's why, it is critical to update software in a timely manner and study reports from Threat Intelligence specialists that provide indicators of compromise and modern hacking techniques.

Source: https://www.group-ib.com/blog/cobalt