بسمه تعالی

بررسی تروجان Milum

گزارش بدافزار

حمله WildPressure نهادهای مرتبط با صنعت را در خاورمیانه هدف قرار می‌دهد. در آگوست ۲۰۱۹ آزمایشگاه Kaspersky، کمپین مخربی که یک تروجان کاملاً فرّار C++ به نام Milum منتشر می‌کرد را کشف کرد. همه قربانیان ثبت شده این تروجان، سازمان‌های واقع در خاورمیانه بودند. برخی از آنها به بخش صنعت مرتبط بودند. موتور اختصاصی تهدید Kaspersky [۱] هیچ شباهت کدی با کمپین‌های شناخته شده مشاهده نکرده است؛ و تا کنون اهداف مشابهی یافت نشده است. در واقع سه نمونه یکسان در یک کشور اتفاق افتاده است. بنابراین ما حملات را هدف قرار داده و در حال حاضر این عملیات را WildPressure نام‌گذاری کرده‌ایم. زمان همه حملات مارس ۲۰۱۹ می‌باشد. در واقع تا قبل از ۳۱ مه ۲۰۱۹ هیچگونه آلودگی ثبت نشده است، بنابراین به نظر نمی‌رسد که تاریخ جعل شده باشد. در این کمپین، اپراتورها از OVH اجاره‌ای و سرورهای خصوصی مجازی Netzbetrieb و یک دامنه ثبت شده توسط سرویس پروکسی ناشناس استفاده می‌کنند.

بدافزار از فرمت JSON[۲] برای داده‌های مربوط به پیکربندی و همچنین به عنوان یک پروتکل ارتباطی C2 از طریق HTTP استفاده می‌کند. در ارتباطات رمزنگاری شده با درخواست‌های HTTP POST، فیلدهای جالبی وجود دارد. یکی از آنها نسخه بدافزار را نشان می‌دهد ۱.۰.۱-. شماره نسخه‌ای از این دست نشان دهنده مرحله اولیه توسعه بدافزار است. فیلدهای دیگر، وجود برنامه‌ها را برای نسخه‌های غیر از C++ پیشنهاد می‌دهد. تنها رمزنگاری پیاده شده الگوریتم RC4 با کلیدهای ۶۴ بایتی متفاوت برای قربانی‌های مختلف است. همچنین توسعه‌دهندگان داده‌های RTTI را درون فایل‌ها قرار دادند. محصولات Kaspersky این بدافزار را Backdoor.Win32.Agent تشخیص دادند.

۱ حمله WildPressure: دسترسی به دستگاه از راه دور

حمله WildPressure، عامل تهدید مانای پیشرفته‌ای (APT) که نهادهای خاورمیانه را هدف قرار می‌دهد و تروجانی منتشر می‌کند که به مهاجمان امکان می‌دهد روی دستگاه آلوده کنترل از راه دور داشته باشند. حملات در آگوست ۲۰۱۹ آغاز شد و با وجود آخرین نسخه‌های منتشر شده همچنان ادامه دارد.

---

[۱] Kaspersky Threat Attribution Engine (KTAE)

[۲] مخفف کلمه **J**ava**S**cript **O**bject **N**otation بوده و یک استاندارد باز است که با ساختاری خوانا برای انسان و هم ماشین، می‌توان اطلاعات و داده‌های مختلف از جمله داده‌های یک دیتابیس را با استفاده از آن، بین عوامل مختلف مثلاً مرورگر کاربر و یک سایت منتقل کرد یا در فضای ذخیره سازی‌ای، آن را ذخیره نمود.

۱-۱ عملکرد WildPressure

- حمله WildPressure تروجان Milum را منتشر می‌کند.
- هنگامی که Milum روی سیستم قربانی بارگذاری شد، مهاجم از قابلیت‌های خود برای مدیریت دستگاه از راه دور و ایجاد کنترل روی سیستم از هر مکانی استفاده می‌کند.
- تروجان Milum می‌تواند دستورات زیادی از طرف مهاجم را اجرا کند؛ مثلاً خود را به نسخه جدید به‌روزرسانی کند، داده‌هایی را جمع‌آوری کرده و به سرور C&C ارسال کند، دستورات را از عملگر خود اجرا کرده و خود را حذف کند.

۱-۲ دلیل نامگذاری Milum

همه تروجان‌های C++ که به عنوان فایل‌های PE مستقل کامپایل شده‌اند، با نام Milum46_Win32.exe شناخته می‌شوند. کلمه «milum» برای نام‌های کلاس C++ درون بدافزار استفاده می‌شود، بنابراین تروجان بعداً نامگذاری می‌شود.

ویژگی بارز دیگر این است که بدافزار بسیاری از توابع فشرده سازی zlib مثل zlibVersion()، inflate() یا deflate() را ایجاد می‌کند. این فشرده سازی برای ارتباط C2 استفاده می‌شود، اما در واقعیت نیازی به ایجاد آنها در یک برنامه مستقل نیست.

فیلدهای پیکربندی JSON به نسخه یا زبان برنامه نویسی محدود نیستند؛ عاملان کمپین از ID قربانی‌ها که در نمونه‌ها بدست آورده‌اند استفاده می‌کنند. در بین آنها، HatLandM30 وHatLandid3 بدست آمده‌اند – که با هیچکدام از آنها آشنا نیستیم. جدول زیر نمونه‌های Milum دارای timestampهای تلفیقی و عنوان PE مشابه اما با IDهای هدف متفاوت را نشان می‌دهد:

ID مشتری	Timestamp (زمان‌سنج)	Milum46_Win32.exe نمونه MD5 hash
839ttttttt	2019.03.09 06:17:19	0C5B15D89FDA9BAF446B286C6F97F535
HatLandid3	2019.03.09 06:17:19	17B1A05FC367E52AADA7BDE07714666B
HatLandM30	2019.03.09 06:17:19	A76991F15D6B4F43FBA419ECA1A8E741

به جای توضیح کلیه فیلدهای پیکربندی، همه آنها در جدول زیر با مشخصات اصلی برای این خانواده بدافزار گردآوری شده‌اند:

زبان برنامه نویسی	C++ با توابع STL برای تجزیه داده‌های JSON و استثناها استفاده می‌شود.

داده‌های پیکربندی	داده‌های JSON با رمزنگاری پایه ۶۴ در منابع PE وجود دارند. شامل timestampها، URLهای C2 و کلید برای ارتباطات، شامل کلیدهای RC4 ۶۴ بایتی
پروتکل شبکه	تروجان داده‌های فشرده JSON در درخواست‌های HTTP POST با gzip، رمزنگاری پایه ۶۴ و RC4 رمزنگاری شده را منتقل می‌کند.
داده‌های Beacon	JSON رمزگذاری شده حاوی بدافزار نسخه ۱.۰.۱، زمان و شناسه مشتری است. همچنین دارای فیلدهای خاصی مثل vt و ext که با زبان برنامه نویسی C++ و پسوند فایل exe مطابقت دارد، می‌باشد. در صورت درست بودن فرضیه، نسخه‌های تروجان غیر از زبان C++ ممکن است برنامه ریزی شود در صورتی که هنوز پیاده سازی نشده است.
ماندگاری	اجرای کلیدهای رجیستری سیستم HKCU autorun و RunOnce
رمزنگاری	رمزگذاری ارتباطی مورد استفاده RC4 با کلید ۶۴ بایت است که در داده‌های پیکربندی ذخیره شده است.
فشرده سازی	برای فشرده سازی، Trojan از یک کد gzip تعبیه شده استفاده می‌کند. به دلایلی توابع gzip از PE تولید می‌شود، اگرچه نمونه‌ها به تنهایی و بدون DLL اجرایی هستند.

۲ دید عمیق‌تر

مشهورترین نمونه در آزمایش به شرح زیر است:

SHA256 a1ad9301542cc23a04a57e6567da30a6e14eb24bf06ce9dd945bbadf17e4cf56
MD5 0c5b15d89fda9baf446b286c6f97f535
Compiled 2019.03.09 06:17:19 (GMT)
Size 520704
Internal name Milum46_Win32.exe

این برنامه در پنجره نوار ابزار مخفی موجود است. توابع مخرب اصلی در یک تهدید جداگانه پیاده سازی شده‌اند. بدافزار Milum داده‌های پیکربندی خود را رمزگشایی می‌کند و در کنار زمان‌بندی، پارامترهای clientid و encrypt_key را برای استفاده در رمزنگاری RC4 بدست می‌آورد.


```
{
    "longwait": "600",
    "shortwait": "30",
    "clientid": "HatLandM30",
    "relays": [
        {
            "key": "nk=a4f3eed19233d0f130335f4f13d90662",
            "url": "http://37.59.87.172/page/view.php"
        },
        {
            "key": "nk=cab282d4e461cee716f42869f0e2796a",
            "url": "http://80.255.3.86/page/view.php"
        }
    ],
    "frelays": [
        {
            "key": "erwersdfddfghftyrt=pk",
            "url": "http://www.upiserversys1212.com/rl.php"
        }
    ],
    "sendresultcount": "30",
    "ext": "",
    "name": "",
    "timeout": "30",
    "encrypt_key": "4kBlRxQx78J6k0Au5S8PDfQqzHF5txqZKbOaSBeV9PPlJbnfWO2stZXqWgIzB8RI"
}
```


شکل ۱ : مثالی از داده‌های پیکربندی رمزنگاری شده. فیلد clientid با نمونه‌های مشاهده شده متفاوت می‌باشد.

در جدول زیر تفاوت بین پارامترهای پیکربندی توضیح داده شده است:

پارامتر پیکربندی	ویژگی های پارامتر
Shortwait	به اندازه چند میلی ثانیه بین چرخه کار ارتباطات C2 متوقف می‌شود.
Clientid	نام هدف منحصر به فرد ASCII
encrypt_key	کلید رمزنگاری RC4 برای ارتباطات C2 مبتنی بر JSON
relays – url	URL کامل برای ارسال دستورات HTTP POST Beacon و GET
relays – key	کلید ASCII منحصر به فرد برای ارتباط با هر C2

مهاجمان می‌توانند با استفاده از کلید B یا b به عنوان شناسه و نام فایل، تروجان را اجرا کنند. در این نمونه Milum همه فایل فرستاده شده به عنوان پارامتر را حذف می‌کند. سپس تروجان دایرکتوری

C:\ProgramData\Micapp\Windows\ را ایجاد کرده و داده‌های پیکربندی خود را برای تولید beacon و فرستادن آن به C2 خود تجزیه می‌کند. برای فرستادن beacon، Milum از درخواست HTTP POST با سه پارامتر ذکر شده در جدول زیر استفاده می‌کند.

پارامترهای Beacon	مقدار پارامترها
md	Id مشتری از پیکربندی، با پیشوند ۰۱۰۱۱ و پسوند پنج کاراکتره تصادفی ASCII
nk	کلید پیکربندی برای برقراری ارتباط با C2، برای هر سرور متفاوت است.
val	فشرده سازی و رمزنگاری داده‌های فرمان JSON

دو پارامتر اول از داده‌های پیکربندی گرفته می‌شوند. پارامتر سوم پس از رمزگشایی، رمزنگاری، غیرفشرده و زیباسازی می‌شود و به شکل زیر است:

```
{
    "version": "1.0.1",
    "vt": "c++",
    "ext": "exe",
    "timestamp": 1559260576, // Thursday, May 30, 2019 11:56:16 PM
    "clientid": "HatLandM30zprqa",
    "command": {
            "id": "-1",
            "type": -1,
            "value": {
                "error_no": "5023",
                "emsg": "error : relay",
                "func": "_response->ProcessResponse",
                "relay": "http://80.255.3.86/page/view.php"
            }
    }
}
```


شکل ۲ : داده JSON beacon رمزگشایی و زیباسازی شده در C2. در این حالت اتصال به سرور اول ناموفق بود.

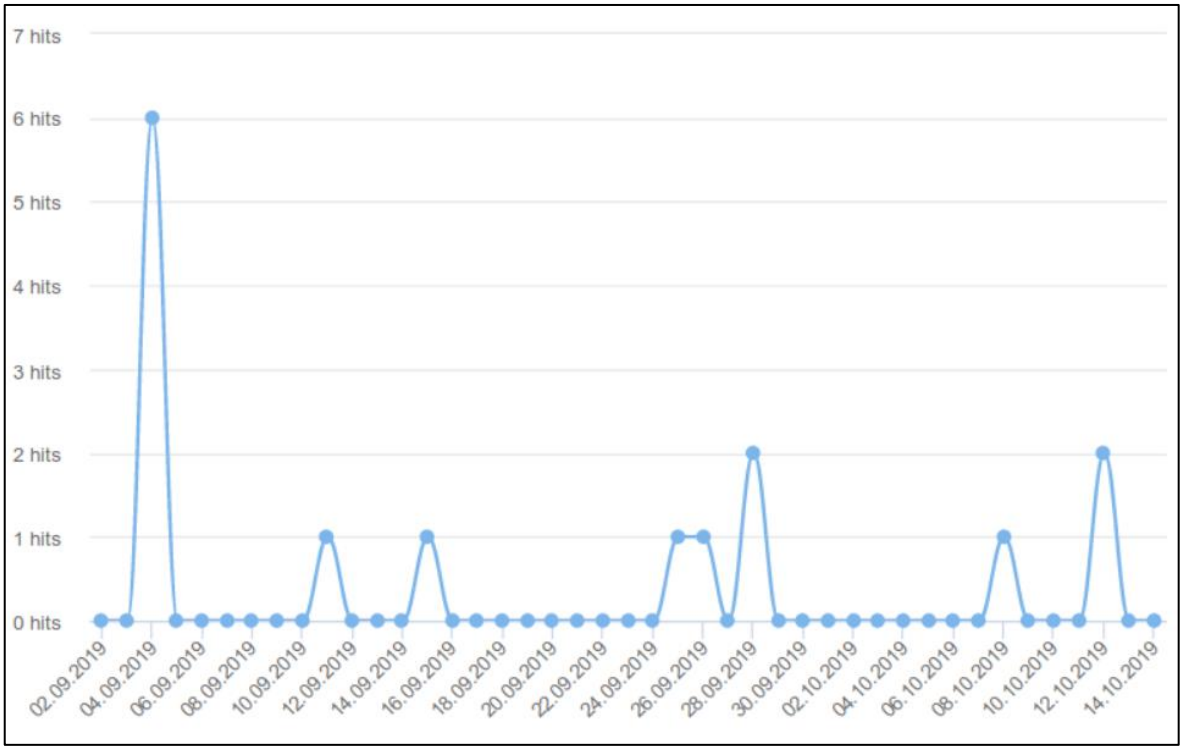
در اینجا چندین مورد قابل ذکر است. در بالا علاوه بر زبان C++، به زبان‌های برنامه نویسی مختلفی اشاره شده است: VT به یک زبان برنامه نویسی و ext به یک پسوند فایل ارجاع داده شده است. با توجه به این مسئله، می‌توان در نظر داشت که ممکن است مهاجمان چندین تروجان داشته باشند که با زبان‌های مختلف نوشته شده و با همان سرور کنترل کار می‌کنند. با توجه به فیلد command، سرورهای کنترل در زمان

تجزیه و تحلیل غیرقابل دسترسی بودند، بنابراین دستوراتی از آنها نداریم. بنابراین نگه دارنده‌های دستور در کد Milum در شکل زیر توضیح داده شده است:

کد	مفهوم	ویژگی‌ها
۱	اجرا	بی درنگ دستور دریافت شده مفسر را اجرا کرده و نتیجه را از طریق pipe بازمی‌گرداند.
۲	Server به client	محتوای دریافتی را در قسمت data در فیلد JSON رمزگشایی کرده و فایل را در مسیر ذکر شده قرار می‌دهد.
۳	Client به server	رمزنگاری فایل مذکور در فیلد path دستور دریافت شده برای ارسال آن
۴	مشخصات فایل	بدست آوردن ویژگی‌های فایل: hidden، read only، archive، executable یا system
۵	پاک کردن	ایجاد و اجرای اسکریپت دسته‌ای برای حذف خودش
۶	نتیجه دستور	دریافت وضعیت اجرای فرمان
۷	اطلاعات سیستم	تایید اعتبار هدف با نسخه ویندوز، معماری (۳۲ یا ۶۴ بیتی)، host و نام کاربری، محصولات امنیتی نصب شده (با درخواست WQL، انتخاب از AntiVirusProduct WHERE displayName <>'Windows Defender')
۸	لیست دایرکتوری	بدست آوردن اطلاعات فایل‌ها در دایرکتوری: hidden، read only، archive، executable یا system
۹	به روزرسانی	نصب نسخه جدید و حذف نسخه قدیمی

۳ نمونه‌های تحت تاثیر حمله

طبق آزمایشات، تروجان Milum حداقل از اواخر ماه مه ۲۰۱۹ منحصراً برای حمله به اهداف در خاورمیانه استفاده می‌شد.



شکل ۷ : تعداد شناسایی حمله برای یکی از نمونه‌ها از سپتامبر ۲۰۱۹

در سپتامبر ۲۰۱۹ دامنه (upiserversys1212[.]com) که یکی از دامنه‌های WildPressure C2 بود، از کار افتاد. اکثریت IPهای بازدید کننده از خاورمیانه بوده و باقی آنها اسکنرهای شبکه، گره‌های خروج TOR یا اتصالات VPN بودند.

Country	Firstseen	Lastseen	Countseen	Tags Host IP
IR	2019-10-28 19:15:49	2019-10-28 19:16:50	1	WildPressure
IR	2019-10-29 07:46:43	2019-10-29 12:08:43	4	WildPressure
IR	2019-10-29 10:56:39	2019-10-29 10:58:00	1	WildPressure
IR	2019-10-30 06:24:20	2019-10-30 08:17:33	42	WildPressure
IR	2019-10-30 11:34:57	2019-10-30 12:35:21	4	WildPressure
IR	2019-10-30 16:50:54	2019-10-30 16:50:54	0	WildPressure
IR	2019-10-30 17:41:49	2019-10-30 17:52:39	2	WildPressure

شکل ۳ : از کار افتادن دامنه C2 آلودگی‌های فعال در خاورمیانه را نشان می‌دهد.

تا به امروز هیچ شباهت قطعی مبتنی بر کد یا قربانی، با عوامل یا مجموعه فعالیت‌های شناخته شده‌ای مشاهده نشده است. کد C++ آنها کاملاً متداول است، در رابطه با داده‌های پیکربندی و بدافزار پروتکل ارتباطی از داده‌های پیکربندی شده با فرمت JSON با رمزگذاری کد پایه ۶۴ استفاده می‌شود که در بخش منبع دودویی ذخیره شده و آن را با توابع Standard Temple Library (STL) تجزیه می‌کند. به هر حال این موارد به اندازه کافی قطعی نبوده و فرض می‌شود که تصادفی هستند. این فعالیت‌ها همچنان تحت نظارت هستند.

۴ نتیجه‌گیری

تا به امروز هیچگونه داده در مورد مکانیسم انتشار Milum مشاهده نشده است. کمپینی که منحصراً اشخاصی را در خاورمیانه هدف قرار می‌دهد (حداقل برخی از آنها مربوط به صنعت هستند)، موضوعی است که به طور خودکار توجه هر تحلیلگر را به خود جلب می‌کند. هر شباهتی باید برحسب اسناد ضعیف در نظر گرفته شود و ممکن است تکنیک‌هایی باشد که از موارد شناخته شده قبلی کپی شده است. در واقع، چرخه «یادگیری از مهاجمین با تجربه تر» در سال‌های اخیر توسط برخی عاملان جدید پذیرفته شده است. این بدافزار علیه یک قربانی خاص طراحی نشده است و ممکن است در سایر عملیات از آن استفاده مجدد شود.

۵ مراجع

[1] https://securelist.com/wildpressure-targets-industrial-in-the-middle-east/96360/