بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

بات نت Lucifer و هدف قرار دادن سیستم‌های ویندوزی

خبر آسیب‌پذیری

شناسه سند ..... Maher_139904092
نوع سند ..... گزارش فنی
شماره نگارش ۰,۱
تاریخ نگارش ۱۳۹۹/۰۴/۰۹
طبقه‌بندی سند ..... عادی

تهران، میدان آرژانتین، ابتدای بلوار بیهقی، نبش خیابان شانزدهم، ساختمان شماره ۱، سازمان فناوری اطلاعات ایران

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ خلاصه

به تازگی بات‌نت جدیدی به نام Lucifer مشاهده شده است که سیستم‌های ویندوزی را مورد هدف قرار می‌دهد. این بات نت پس از آلوده کردن سیستم، آن را توسط رباتی به یک کلاینت cryptomining تبدیل کرده و از این طریق می‌تواند حملات انکار سرویس (DDoS[۱]) توزیع شده را آغاز کند.

نویسنده بدافزار، این ربات را Satan DDoS نام‌گذاری کرده است اما محققان ۴۲ Palo Alto Network's Unit، به آن لقب Lucifer داده‌اند زیرا بدافزار دیگری نیز با همین نام وجود دارد. (Satan Ransomware)

در ۲۹ام ماه می ۲۰۲۰، محققانِ Unit 42، نوع جدیدی از بدافزار ترکیبی[۲] cryptojacking را کشف کردند که آسیب‌پذیری با شناسه "CVE-2019-9081"را اکسپلویت می‌کند. بررسی‌ها نشان می‌دهد بدافزار Lucifer قادر به انجام حملات DDoS و همچنین اکسپلویت هاست‌های آسیب‌پذیر ویندوز می‌باشد.

[۱] denial-of-service

[۲] hybrid

۲ جزئیات فنی

کارشناسان هنگام بررسی مؤلفه‌های اکسپلویتِ آسیب‌پذیری با شناسه "CVE-2019-9081"، (آسیب‌پذیری بحرانی RCE که بر روی یک مؤلفه فریمورک وب Laravel تأثیر می‌گذارد) متوجه این باتنت شدند. اولین نمونه از ربات Lucifer، در ۲۹ ماه می ۲۰۲۰ کشف شد.

Lucifer بسیار قدرتمند است، این باتنت علاوه بر آن که می‌تواند XMRig را جهت cryptojacking Monero حذف کند[۳]، قادر است از طریق اکسپلویت آسیب‌پذیری‌های مختلف، نظارت بر سرور کنترل و فرمان(C2[۴]) را نیز برعهده گرفته و حملات EternalBlue, EternalRomance و DoublePulsar را علیه اهداف آسیب‌پذیر اینترانت اجرا کند. Lucifer همچنین می‌تواند ماشین‌های با پورت‌های۱۳۵ (RPC) TCP و ۱۴۳۳ (MSSQL) را اسکن نماید. این باتنت قادر به حذف XMRig Monero بوده و شامل ماژول DDoS می‌باشد و مکانیزم خود را با اکسپلویت آسیب‌پذیری‌های متعدد و اجرای حملات جدی پیاده‌سازی خواهد کرد.

در ابتدا این بدافزار به منظور آلوده کردن هاست‌های خارجی[۵]، یک آدرس IP غیرخصوصی تولید کرده و سپس قربانی که به طور تصادفی انتخاب شده است را با درخواست‌هایHTTP بر روی تعدادی از پورت‌ها مورد بررسی قرار می‌دهد.

جدول ۱: آسیب‌پذیری‌های اکسپلویت شده توسط این باتنت

شناسه آسیب‌پذیری	وضعیت
CVE-2014-6287	HFS در پاسخ HTTP یافت می‌شود.
CVE-2018-1000861	Jetty در پاسخ HTTP یافت می‌شود.
CVE-2017-10271	Servlet در پاسخ HTTP یافت می‌شود.

[۳] dropping

[۴] command and control

[۵] external hosts

ThinkPHP remote code execution (RCE) vulnerabilities CVE-2018-7600 CVE-2017-9791 CVE-2019-9081 PHPStudy Backdoor remote code execution (RCE)	هیچ کلیدواژه‌ای یافت نمی‌شود.

مهاجم می‌تواند پس از به خطر افتادن سیستم قربانی توسط این باتنت، دستورات دلخواه را بر روی دستگاه آلوده اجرا کند. کارشناسان دریافتند که Lucifer قادر است که هم اینترنت و هم اینترانت هاست‌های ویندوز را مورد هدف قرار دهد.

شایان ذکر است که این بدافزار می‌تواند توسط یک دیکشنری حملات بی‌رحمانه خود را آغاز کند! که در این حملات، بدافزار متکی به یک دیکشنری با ۷ نام کاربریِ " "SQLDebugger" "kisadmin" "su" "SA" "sa" "mssql"" و "۱۴۳۳Chred" و صدها گذرواژه می‌باشد.

۳ نرم افزارهای تحت تأثیر

نرم‌افزارهای آسیب‌پذیر عبارتند از:

- Rejetto HTTP File Server
- Jenkins
- Oracle Weblogic
- Drupal
- Apache Struts
- Laravel framework
- Microsoft Windows

۴ توصیه امنیتی

با توجه به اهمیت این مسئله، توصیه می‌شود هر چه سریع‌تر به روزرسانی‌ها و وصله‌های امنیتی نرم‌افزارهای تحت تأثیر را اعمال کرده و همچنین جهت جلوگیری از حملاتی که از طریق دیکشنری صورت می‌پذیرند، لازم است از گذرواژه‌های قوی استفاده کنید.

۵ جمع‌بندی

Lucifer باتنتی مخرب است که ترکیب جدیدی از cryptojacking و نوعی بدافزار DDoS می‌باشد که منجر به اکسپلویت آسیب‌پذیری‌های قدیمی و انجام فعالیت‌های مخرب بر روی سیستم‌عامل‌های ویندوز می شود، کاربران جهت حفظ امنیت سیستم خود، باید هر چه سریع‌تر اقدامات لازم را در این خصوص مبذول نمایند.

۶ منابع خبر

[1] https://securityaffairs.co/wordpress/105232/malware/lucifer-ddos-botnet-windows.html

[2] https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/