بسمه تعالی

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

حمله باتنت KashmirBlack به سیستم‌های مدیریت محتوای معروف

هشدار

شناسه سند ..... MaherReport_13990807.
نوع سند ..... گزارش فنی
شماره نگارش ۰,۱
تاریخ نگارش ۱۳۹۹/۰۸/۰۷
طبقه‌بندی سند ..... عادی

تهران، خیابان بهشتی، نرسیده به قائم مقام فراهانی، پلاک ۲۶۷، سازمان فناوری اطلاعات ایران
(۰۲۱) ۴۲۶۵۰۰۰۰
(۰۲۱) ۴۲۶۵۰۰۰۰
cert.ir

فهرست مطالب

۱ مقدمه

بر اساس گزارش تیم Imperva، باتنت KashmirBlack به‌طور گسترده پلتفرم‌های مدیریت محتوای پرکاربرد را آلوده می‌کند. این باتنت با سوءاستفاده از چندین آسیب‌پذیری شناخته شده بر روی سرور قربانی، بطور میانگین میلیون‌ها حمله را هر روزه و بر روی چندین هزار قربانی در بیش از ۳۰ کشور انجام می‌دهد.

در این گزارش محققان Imperva پیاده‌سازی و سیر تکامل این باتنت خطرناک را از ماه نوامبر ۲۰۱۹ تا پایان ماه می ۲۰۲۰ میلادی بررسی کرده‌اند. در این تحقیق چگونگی استفاده باتنت از سرویس‌های ابری همچون Github، Pastebin و Dropbox به منظور کنترل و مخفی کردن عملیات باتنت و چگونگی نفوذ آن به ماینر ارزهای دیجیتالی و deface یک سایت گفته شده است. همچنین نشانه‌های حمله در اینجا نمایش داده شده است. جدول ۱ مشخصات این باتنت پیچیده را نمایش می‌دهد.

جدول ۱- مشخصه‌های باتنت KashmirBlack

مشخصه ها	توضیحات
زمان شروع فعالیت	نوامبر ۲۰۱۹
مدت فعالیت	حداقل ۱۱ ماه و همچنان ادامه دارد.
پلتفرم‌های تاثیر حمله	پلتفرم‌های مدیریت محتوای پرکاربرد مانند: WordPress, Joomla!, PrestaShop, Magneto, Drupal, Vbulletin, OsCommerence, OpenCart, Yeager
کشورهای مورد حمله	بیش از ۳۰ کشور، عمدتا در ایالات متحده امریکا
نوع حمله	آپلود فایل بدون محدودیت، اجرای کد از راه دور، پیمایش مسیر، Brute Force یا Account takeover
تعداد بات‌ها	۲۸۵ مورد IP مشاهده شده اما به‌نظر می‌رسد که چند صد هزار مورد باشد.
نحوه گسترش باتنت	استفاده از زیرساخت های پیچیده و well-designed برای گسترش

.

۲ زیر ساخت باتنت

شکل۱ نمایش ساده‌ای از پیچیدگی باتنت و موجودیت‌های درگیر در عملیات باتنت را نشان می‌دهد. رنگ هر کدام از موجودیت‌ها معین کننده مشخصه‌های آن است. بدین ترتیب که رنگ قرمز برای سرویس‌های آلوده‌ای است که توسط مالک باتنت درست شده، رنگ نارنجی قربانیان مورد سوءاستفاده واقع شده و رنگ سبز هم نشان دهنده سیستم مدیریت محتوای آلوده نشده است که هدف حمله می باشند. در ادامه توضیحاتی مبنی بر هر کدام از موجودیت‌ها ارائه شده است:

- سرور C&C: یک ماشین مرکزی است که وظیفه کنترل ماشین‌هایی را برعهده دارد که اجزای باتنت را تشکیل می دهند.
- Repository A : اسکریپت‌های باتنت آلوده را به منظور ارتباط با سرور C&C نگهداری می‌کند.
- Repository B : ملزومات مرتبط با اکسپلویت و payloadها را نگهداری می‌کند.
- Spreading bot : به طور مداوم با سرور C&C در ارتباط است تا دستور العمل‌های حمله به قربانیان دیگر را دریافت نماید. در صورت موفقیت‌آمیز بودن حمله، بات گزارشی مبنی بر آن که قربانی جدید به ‘Pending bot’ تبدیل شده است به سرور C&C ارسال می‌کند.
- Pending bot : منتظر سرور C&C می‌ماند تا نقش این بات جدید را در سناریو حمله مشخص کند.

شکل ۱- زیر ساخت باتنت KashmirBlack

۳ شروع فعالیت باتنت

بر اساس تحقیقات تیم Imperva عملیات باتنت KashmirBlack در نوامبر ۲۰۱۹ میلادی شروع شد. این تیم دو سرنخ دارند که نشانه صحت ادعای آنهاست. اولین سرنخ، از داده‌های شرکت Imperva مبنی بر تلاش‌هایی برای اکسپلویت برخی از مشتریان Imperva سرچشمه گرفته است. شواهدی از تلاش‌هایی برای اکسپلویت آسیب‌پذیری PHPUnit RCE با شناسه CVE-2017-9841 توسط باتنت KashmirBlack در اوایل نوامبر وجود داشته است و سرنخ دوم مربوط به تاریخ یکی از اکسپلویت‌ها (۶ نوامبر ۲۰۱۹ میلادی) در ‘repository B’ است.

با توجه به یافته‌های Imperva، باتنت در ابتدا کوچک بوده اما پس از رشد مدوام در طول ماه‌ها تبدیل به یک غول پیچیده شده است که همه روزه توانایی حمله به هزاران سایت را دارد. بزرگترین تغییر ساختار این باتنت در ماه می سال جاری میلادی رخ داده است، زمانی که باتنت موجودیت جدید ‘repository A load balancer’ را به ساختار خود اضافه کرد و چندین repositories برای گسترش ‘repository A’ و ‘repository B’ افزود. امروزه، باتنت KashmirBlack توسط یک سرور C&C مدیریت می‌شود و بیش از ۶۰ سرور قربانی در زیرساخت خود دارد.

۴ هدف باتنت

باتنت KashmirBlack با هدف پیدا کردن سایت‌هایی که نرم‌افزارهای منسوخ شده دارند، اینترنت را پایش کرده و گسترش می‌یابد و سپس با اکسپلویت آسیب‌پذیری‌های شناخته شده، سایت هدف و سرورهای آن را تحت تاثیر قرار می‌دهد.

برخی از سرورهای هک شده در استخراج ارزهای دیجیتالی و اسپم کاربرد دارند اما برخی دیگر در حمله به سایت‌های دیگر و سرپا نگه داشتن باتنت ایفای نقش می‌کنند. از نوامبر ۲۰۱۹ میلادی این باتنت از ۱۶ آسیب‌پذیری مختلف استفاده کرده است. این آسیب‌پذیری‌ها به باتنت KashmirBlack این اجازه را می‌دهند که به سیستم‌های مدیریت محتوا از قبیل: Drupal, Magneto, PrestaShop, Joomla, WordPress, OpenCart, osCommerce, vBulletin و Yeager حمله کنند .در برخی از اکسپلویت‌ها فقط به سیستم مدیریت محتوای سایت حمله شده اما در برخی دیگر به المان‌های داخلی و کتابخانه ها نیز حمله می‌شود.

از ۱۶ آسیب‌پذیری مذکور ، تنها یک اکسپلویت مربوط به آسیب‌پذیری PHPUnit RCE با شناسه CVE-2017-9841 است که به مهاجم این اجازه را می‌دهد تا کدهای php را به منظور اجرا در سرور قربانی تزریق نماید و منجر به تبدیل سایت قربانی به ‘spreading bot’ شود. ۱۴ آسیب‌پذیری در جریان آلوده‌سازی، منجر

به تبدیل سایت قربانی به ‘pending bot’ می‌شود که در ادامه لیست شده است و یک مورد آسیب‌پذیری باقی‌مانده با استفاده از ضعف WebDAV که در اینجا شرح داده شده است منجر به Defacement می‌شود.

- JQuery file upload vulnerability – CVE-2018-9206
- ELFinder Command Injection – CVE-2019-9194
- Joomla! remote file upload vulnerability
- Magneto Local File Inclusion – CVE-2015-2067
- Magento Webforms Upload Vulnerability
- CMS Plupload Arbitrary File Upload
- Vulnerability – CVE-2015-7571 and many unregistered
- Multiple vulnerabilities including File Upload & RCE for many plugins in multiple platforms here
- WordPress TimThumb RFI Vulnerability – CVE-2011-4106
- Uploadify RCE vulnerability
- vBulletin Widget RCE – CVE-2019-16759
- WordPress install.php RCE
- WordPress xmlrpc.php Login Brute-Force attack
- WordPress multiple Plugins RCE (see full list in appendix A)
- WordPress multiple Themes RCE (see full list in appendix B)

۵ راه‌کار

مدیر سایت بایستی اطمینان حاصل نماید که فایل‌های CMS و ماژول‌های سوم شخص همیشه به‌روز بوده و به طول کامل پیکربندی شده باشند. علاوه بر این، از دسترسی به فایل‌های حساس و مسیرهایی از قبیل install.php, wp-config.php و eval-stdin.php جلوگیری شود. پیشنهاد می‌شود که از رمزعبورهای قدرتمند و خاصی استفاده گردد چون این رمزعبورها اولین نقطه دفاعی در برابر حملات بروت فورس هستند. همچنین به دلیل گسترش جرایم رایانه‌ای و افشای آسیب‌پذیری‌های روز افزون توصیه می‌شود برای اطمینان کامل از امنیت سایت خود از WAF استفاده نمایید.

در صورتی که سرور شما توسط بات نت KashmirBlack آلوده شده باشد، بایستی اقدامات ذیل را انجام دهید:

- توقف پروسس‌های آلوده
- حذف فایل‌های آلوده
- حذف تسک‌های زمانبندی شده (Cron Jobs) مشکوک و ناآشنا
- حذف پلاگین و تم‌های استفاده نشده

۶ منبع

1. https://www.imperva.com/blog/crimeops-of-the-kashmirblack-botnet-part-i
2. https://www.imperva.com/blog/crimeops-of-the-kashmirblack-botnet-part-ii/