禪

پس از نیمه شب (Aftermidnight) و قاتل (Assassin)

باید در انتظار گونههای جدیدتر و خطرناکتری از بدافزارها باشیم؟

Remote control & subversion malware systems
'After Midnight' and 'Assassin'
WikiLeaks

در چند روز گذشته دنیای امنیت و به ویژه فضای سایبری تحت تاثیر یکی از خطرناکترین باجافزارهای ممکن قرار گرفت. باجافزاری که ضمن قفل کردن فایلهای کاربران این پتانسیل را داشت تا همانند یک کرم اینترنتی رفتار کرده و خود را تکثیر کند . اما اسنادی که به تازگی منتشر شدهاند حکایت از این موضوع دارند که در آینده نزدیک ممکن است با گونههای دیگری از بدافزارها روبرو شویم .

در حالی که سوییچ مرگ موفق شد، در یک بازه زمانی کوتاه مانع آلوده شدن کاربران شود، اما این پتانسیل را نداشت تا از گسترش این باجافزار ممانعت به عمل آورده و مهمتر از آن موفق نشد دامنه فعالیتهای مخرب این باجافزار را بهطور کامل متوقف کند . هکرها با یک تغییر نام ساده دامنه موفق شدند یکبار دیگر فعالیت خود را از سر گرفته و بر پایه جدیدترین گزارش نزدیک به 200 هزار سامانه کامپیوتری را در 150 کشور جهان آلوده سازند . حال تصور کنید از این تعداد سامانه آلوده تنها یک سوم از آنها حاضر شوند باج مربوطه را پرداخت کنند . سود به دست آمده انگیزه لازم را در اختیار هکرها قرار میدهد تا به شکل جدیدتری به کار خود ادامه دهند .

مطلب پیشنهادی

WannaCry—New Variants Detected!

[illegible]

[illegible] **WannaCry** [illegible]

[illegible] (Aftermidnight) [illegible] (Assassin) [illegible] AfterMidnight [illegible] Dll [illegible] Gremlins [illegible] Gremlins [illegible] AlphaGremlin [illegible] Aftermidnight [illegible]

[illegible]

[illegible] WannaCry [illegible]

[illegible] **WannaCry** [illegible] «[illegible]»

[illegible] Assassin [illegible] LAN [illegible]

[illegible]

[illegible]

[illegible]

[illegible] WannaCry [illegible]

نمونهای از این موارد است .

مطلب پیشنهادی

Botnet Mines Cryptocurrency

استخراج ارز مجازی توسط Bondnet

غارت ارزهای مجازی با باتنت

سیسکو نیز یک آسیبپذیری بحرانی را در سوییچهای خود وصله کرد

در همین ارتباط شرکت سیسکو نیز موفق شد یک آسیبپذیری بحرانی را در سوییچهای خود ترمیم کند . این آسیبپذیری نیز از سوی آژانسهای دولتی مورد استفاده قرار میگرفت . در حالی که نزدیک به دو ماه پیش (مارس) شرکت سیسکو در ارتباط با این آسیبپذیری به مشتریان خود هشدار داده بود، اما این شرکت به تازگی آسیبپذیری فوق را ترمیم کرده است . آسیبپذیری موجود روی سوییچهای سیسکو به هکرها اجازه میداد از راه دور به شبکهها نفوذ کنند . هکرها از طریق یک ارتباط Telnet قادر بودند با دستگاه آسیبپذیر ارتباط برقرار کرده و در ادامه دستور مبتنی بر پروتکل مدیریت خوشه (CMP) را روی آن اجرا کنند . این آسیبپذیری به هکرها اجازه میداد کنترل دستگاه را به دست آورده و آنرا راهاندازی مجدد کنند . شرکت سیسکو در بیانیهای گفته است که به این آسیبپذیری از یک تا ده نمره 9.8 را میدهد . شرکت سیسکو به مدیران شبکهها توصیه کرده است سرویس Telnet را غیر فعال کنند .

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
22:46 - 26/02/1396
برچسب:
امنیت - ویندوز - Aftermidnight - Assassin - سیسکو - باجافزار - آسیبپذیری

نشانی
:https://www.shabakeh-mag.com/security/7905/%D8%A8%D8%A7%DB%8C%D8%AF-%D8%AF%D8%B1-%D8%A7%D9%86%D8%AA%D8%B8%D8%A7%D8%B1-%DA%AF%D9%88%D9%86%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%AC%D8%AF%DB%8C%D8%AF%D8%AA%D8%B1-%D9%88-%D8%AE%D8%B7%D8%B1%D9%86%D8%A7%DA%A9%E2%80%8C%D8%AA%D8%B1%DB%8C-%D8%A7%D8%B2-%D8%A8%D8%AF%D8%A7%D9%81%D8%B2%D8%A7%D8%B1%D9%87%D8%A7-%D8%A8%D8%A7%D8%B4%DB%8C%D9%85%D8%9F