禪

بیگانه ای پرسه می زند

ابزار امنیتی ویژهای برای شکار سرورهای کنترل و فرماندهی عرضه شد

Malware Hunter
Finding the Command & Control Centers of Botnets across the Globe.

10+ RATs **3,000+** C2s identified **24/ 7** Coverage

در حملات هکری مجرمان سایبری بدافزارهای خود را بهگونهای طراحی میکنند که در ابتدا سامانههای کامپیوتری را آلوده کند و در ادامه از طریق یک سرور کنترل و فرماندهی با هکرها در ارتباط باشند . هکرها از طریق این مرکز کنترل و فرماندهی دستورات لازم را برای بدافزار ارسال میکنند . باتنتها و باجافزارها بهشکل گستردهای از این سرورها استفاده میکنند . حال اگر بتوانیم مانع برقراری این ارتباط شویم، در واقع موفق شدهایم ارتباط میان هکر و بدافزار را از میان ببریم . در چنین حالتی شانس ما برای مقابله با بدافزارها دوچندان خواهد شد . سرویس Malware Hunter که به شکارچی بدافزارها معروف شده برپایه همین ایده طراحی شده است .

سرویس فوق به شرکتها و سازمانها اجازه میدهد کانال ارتباطی میان بدافزارها و سرورهای کنترل و فرماندهی را مسدود کنند . شرکت Recorded Future که در زمینه شناسایی تهدیدات امنیتی از طریق الگوریتمهای یادگیری ماشینی به فعالیت اشتغال دارد، با همکاری موتور جستوجوگر شادون موفق شده است این سرویس آنلاین را طراحی کند . سرویس فوق بهطور مستمر در سطح اینترنت به جستوجو پرداخته تا پانلهای کنترلی متعلق به دهها برنامه RAT (سرنام Remote Access Trojan) را شناسایی کند .

مطلب پیشنهادی

[redacted]

[redacted]

XtremeRAT ، Gh0st RAT، DarkComet، njRAT، ZeroAccess [redacted] (Command-and- Control [redacted]) (C&C) [redacted] IP [redacted].

[redacted]

[redacted]

[redacted]

[redacted] Malware Hunter [redacted] 5700 [redacted] Gh0st [redacted] 2009 [redacted] Research Future [redacted] RAT [redacted].

Cerber

:□□□□ □□□□
□□□□□
:□□□□□ □□□□□
06:05 - 15/04/1396
:□□□□□
□□□□□□ - Malware Hunter - Malware Hunter □□□□□ - □□□□□□□ □□□ - □□ □□ □□□ - □□□□ □□□□□ - □□□
□□□□□ □□□ - □□□□□□□□□

□□□□□
https://www.shabakeh-mag.com/security/8451/%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1-%:□□□□
D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-
%D9%88%DB%8C%DA%98%D9%87%E2%80%8C%D8%A7%DB%8C-
%D8%A8%D8%B1%D8%A7%DB%8C-%D8%B4%DA%A9%D8%A7%D8%B1-
%D8%B3%D8%B1%D9%88%D8%B1%D9%87%D8%A7%DB%8C-
%DA%A9%D9%86%D8%AA%D8%B1%D9%84-%D9%88-
%D9%81%D8%B1%D9%85%D8%A7%D9%86%E2%80%8C%D8%AF%D9%87%DB%8C-
%D8%B9%D8%B1%D8%B6%D9%87-%D8%B4%D8%AF