Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs

Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs

Script kiddies and online criminals around the world have reportedly started exploiting NSA hacking tools leaked last weekend to compromise hundreds of thousands of vulnerable Windows computers exposed on the Internet.

Last week, the mysterious hacking group known as Shadow Brokers leaked a set of Windows hacking tools targeting Windows XP, Windows Server 2003, Windows 7 and 8, and Windows 2012, allegedly belonged to the NSA's Equation Group.

What's Worse?

Microsoft quickly downplayed the security risks by releasing patches for all exploited vulnerabilities, but there are still risks in the wild with unsupported systems as well as with those who haven't yet installed the patches.

Multiple security researchers have performed mass Internet scans over the past few days and found tens of thousands of Windows computers worldwide infected with **DoublePulsar**, a suspected NSA spying implant, as a result of a free tool released on GitHub for anyone to use.

Security researchers from Switzerland-based security firm Binary Edge performed an Internet scan and detected more than 107,000 Windows computers infected with DoublePulsar.

A separate scan done by Errata Security CEO Rob Graham detected roughly 41,000 infected machines, while another by researchers from Below0day detected more than 30,000 infected machines, a majority of which were located in the United States.

The impact ?

DoublePulsar is a backdoor used to inject and run malicious code on already infected systems, and is installed using the **EternalBlue** exploit that targets SMB file-sharing services on Microsoft's Windows XP to Server 2008 R2.

Therefore, to compromise a machine, it must be running a vulnerable version of Windows OS with an SMB service expose to the attacker.

Both DoublePulsar and EternalBlue are suspected as Equation Group tools and are now available for any script kiddie to download and use against vulnerable computers.

Once installed, DoublePulsar used hijacked computers to sling malware, spam online users, and launch further cyber attacks on other victims. To remain stealthy, the backdoor doesn't write any files to the PCs it infects, preventing it from persisting after an infected PC is rebooted….[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).

Même si remplir un formulaire de déclaration à la CNIL est gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés.
Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données.

Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
formateur n°93 84 03041 84

Réagissez à cet article

Source : *Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs*