ZERODAYLAB®

Understanding the impact of Zero Day attacks

On any given day, nation-states and criminal hackers have access to an entire arsenal of zero day vulnerabilities — undocumented and unpatched software flaws that can be used to silently slip past most organisations' digital defences.

It's no secret, nor has it been for quite some time, that most national governments and criminal organisations have a full inventory of zero day attacks at their disposal.

Attackers will be on a site for an average of 101 days before being detected.*

This means that powerful entities can readily access your systems without your approval, and without leaving a trail. But even if they are somehow discovered, the hackers can just move on to the next zero day attack. They're expensive, but they're also plentiful.

Besides, by the time they've been detected, the intruders will likely already have everything they need, whether it's intellectual property, credit card data, healthcare records, and/or any other sensitive information you're trying to protect.

*FireEye M Trends 2018

ZERODAYLAB®

The Goal of the Zero Day Attack

So, if it's understood that zero day attacks are ubiquitous, and your organisation is likely to be an eventual target, the question becomes: once a zero day attack is executed, what happens next?

The first thing the attackers do is look for ways to expand their access, usually by installing remote access kits, key loggers and rootkits. Their goal is to extract credentials in order to achieve lateral motion throughout the network.

To accomplish this, the hackers search for encryption keys, passwords, certificates, Kerberos tickets, and the hashes of privileged accounts that can be found on compromised machines. Often the attackers will quietly monitor and record activity on the systems and then use the information to expand their control of the IT environment.

It is called the "land and expand" cyber-attack for a reason and the entire activity can be completed in only 15 minutes.

However, that's just the attack phase. The intruders will nest on the network for a much longer period of time. According to many leading analysts, zero day exploits persist for an average of 101 days* before being discovered; obviously, more than enough time to map the network and extract valuable data at will.

*FireEye M Trends 2018

ZERODAYLAB®

Prevention is Not an Option - Early Detection is Critical

In 2018, 38%* of organisations learned of a breach from an outside entity, an increase on the previous year.

The world is increasingly interconnected. Business and financial institutions continue to adopt web-based systems and with data migrating to mobile technology platforms, making the risks of cybercrime become ever more real.

The number of Threat Actors has never been greater. Criminals remain determined to pursue financial gain through Fraud and Identity Theft. The combination of "Hactivists'" intent on defacing web servers, competitors stealing Intellectual Property, together with complex Government and industry regulations, the challenge to protect your critical assets from attack can seem overwhelming.

Many organisations employ a layered method to security, implementing a variety of best of breed security solutions, reducing reliance on any one specific vendor or platform. However, this heterogeneous approach poses a problem; there is no inherent way of normalising, correlating and analysing security events across all technologies. Log management, event monitoring, and security information and event management (SIEM) solutions help defend against attacks by aggregating data, but without contextual information providing real-time threat analytics, your security team lacks the intelligence it needs for breach prevention.

*FireEye M Trends 2018

ZERODAYLAB®

ZeroDayLab Next Generation SOC Services

ZeroDayLab provides the next level of intelligence that MSSPs cannot provide. Whether you currently maintain your critical IT assets within a SOC (Security Operations Centre or are planning to transition to one, our Next Generation SOC Services are designed to enable or augment your current technology to help defend against today's malicious Threat Actors.

Where an organisation is subject to complex legal and compliance regulations, or needs to gain greater visibility of the vast quantities of data generated, our Next Generation SOC helps protect infrastructure, gain deeper analysis and ensure compliance.

ZeroDayLab's tailored approach to SOC enablement allows you to pick and choose security services best aligned to your current security posture, whilst remaining agile within a dynamic threat landscape. Cost-effective, efficient on-boarding enables you to move seamlessly from a simple, yet robust monitoring system to a full-blown Cyber Security solution used by Government agencies, public sector departments and commercial companies worldwide.

360 degree Threat Intelligence from ZeroDayLab will provide you with the most up-to-date defence against today's and tomorrow's threat actors whilst providing you with the up-to-date cyber-intelligence to make strategic business decisions to protect your valued assets and reputation.

ZERODAYLAB®

UfRSqcXcpmB_RJ_`=

We maximise ROI by delivering value for money services of the highest and consistent quality.

Mspqcptgacq

- Tsjlcp_`gjgrR?qqcqqkclrmdBcqirmn*Qcptcpq_lbGldp_qrpsarspc
- Nclcrp_rgmlRcqrglemd_jjGlrcpl_j-Cvrcpl_jUc`?nnjga_rgmlq_lbGldp_qrpsarspc
- @pm_bQcaspgrRPctgcu&?pafgrcarspc_lbGldp_qrpsarspc'
- QmspacAmbcPctgcuq
- Dgpcu_jj?sbgrq
- Bcqirmn_lbQcptcp@sgjbPctgcuq
- @jmaiaf_gl?nnjga_rgmlQcaspgrR?sbgrq
- Bgegr_jDmpclqga?l_jRqgq
- QcaspgrR?u_pclcqqNpmep_kkcq
- QcaspgrRRp_glgledmpBctcjmncpq+QcaspcAmbgleQafmmj*A@R*Mljglc?qqcqqkclr
- Npc+@pc_afGlagbclrPcqnmlqc$Psl`mmiRp_glgle
- Nfgqfgle Pcqgjgclac Npmep_kkcq
- @cqnmicQclgmpCvcasrgtcQcaspgrRRp_glgl
- PcbRc_kRcqrgle
- NAGBQQPckcbg_rgmlQsnnmpr
- E_n?l_jRqgqrmGQM*NAGBQQ*QQ?C/4&/6'*
- IGQR* EBNP
- 14.ßPctgcuq&AR`cpPgqi?qqcqqkclr'
- Tgprs_jB_r_Npmrcargml Mddgacp
- Tgprs_jGldmpk_rgmlQcaspgrRK_l_ecp
- GQM-IGQR-CSEBNPQr_lb_pbq?jgelkclr
- Glrcpl_j?sbgrq
- QCPK+Qsnnjgcpct_js_rgmlPgqiK_l_eckclr
- AR`cpRfpc_rGlrcjjgeclac+Bccn$B_piUc`
- Qcpmrcargtc Kmlgrmpgle&K_l_ecbQMA'
- Qcaspgr RPgqiRp_glgledmp?egjcBctcjmncpc
- XcpmB_RPcqnmlqc+Glagbclr Pcqnmlqc Pctgcu $Bgegr_jDmpclqgaqRp_glgle

ZERODAYLAB®

Passionate About Total Security Management

Europe Headquarters:

ZeroDayLab Ltd
Suite 303, 150 Minories,
London,
EC3N 1LS, UK
Phone: +44 (0)207 979 2067

North America Headquarters:

ZeroDayLab LLC
3524 Silverside Road, Suite 35B
Wilmington, DE
19810-4929, USA
Phone: 1-302-498-8322

Amsterdam | Manchester | Edinburgh | Dublin | Brighton & Hove | Bangalore

www.zerodaylab.com | www.zerodaylab.nl | info@zerodaylab.com