CyberGuard Technologies

Proactive Cyber Defence Report

April 2019

It has been a busy month with ransomware back in the headlines and a large-scale attack targeting users of both Office 365 and Gmail.

Throughout March, CyberGuard's Incident Response Team have seen a sharp rise in Office 365 compromises. So much so, we issued an alert to all customers – see here: https://ogl-group.co.uk/t/4FMO-IWGE-501A2PHH24/cr.aspx.

The attackers used legacy protocols such as IMAP and POP to access mail accounts. Interestingly this type of attack worked even if you had two-factor authentication turned on.

Analysis from cyber security firm, Proofpoint, unearthed the fact that around 60% of all Microsoft Office 365 and G Suite tenants have been targeted using IMAP-based password-spraying attacks. As a direct result, approximately 25% of G Suite and Office 365 tenants that were attacked also experienced a successful breach.

These numbers are large, and this really does highlight the importance of setting strong unique passwords, always turning on two-factor authentication (not helpful in this instance) and, adding monitoring to alert you of any suspicious behaviour.

Sticking with Microsoft, a report has found that Microsoft products were the most targeted during 2018. Eight out of the top ten vulnerabilities last year affected their products. Phishing, Remote Access Trojans (RAT) and exploit kits were amongst the methods affecting them.

The report, published by Recorded Future, observed that the use of exploit kits has dropped due to the use of more targeted attacks and a shift towards the more secure browsers and specific victim targeting.

In 2017, Microsoft products were affected by seven out of ten vulnerabilities. Adobe Flash Player was also heavily targeted in 2015 and 2016.

Two large scale ransomware attacks have recently been in the news. LockerGoga made headlines last week after targeting Norsk Hydro, forcing the company to shut down or isolate several plants and send several more into manual mode. According to an update by the company that incident has so far cost Norsk Hydro at least $40 million in the last week.

But the ransomware was around well before this incident, spotted as early as 24 January in an attack against engineering consultancy, Altran. They said in a statement that they were hit by a cyber-attack that impacted operations in "some European countries."

Two other manufacturing companies, Hexion and Momentive, have also been hit by the ransomware, according to reports. So far, researchers at Palo Alto Networks said they have identified 31 ransomware samples that are similar in behaviour and code to the initial variant. The initial access is still unknown and was thought to be from a phishing email, but no evidence has been found, although could be from stolen credentials logging into a VPN or remote desktop session.

This variant of ransomware does not use any propagation techniques such as Wannacry, and because of the encryption used, it is also relatively slow to encrypt file points. Engineers from McAfee have confirmed the use of a valid certificate, which is why this software evades some security products.

If you have the ability to query computers on your network, you can scan them for these indicators of compromise, although new variants will be produced.

IOCs

Hash:

```
73171ffa6dfee5f9264e3d20a1b6926ec1b60897
```

File names:

```
worker
worker32
bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f_wQkb8SOVnc
.bin
svch0st.5817.exe
svch0st.11077.exe
```

Associated email addresses:

```
CottleAkela@protonmail.com
QyavauZehyco1994@o2.pl
```

Magento, a popular content management system (CMS), has released a new version of its software, addressing a number of security vulnerabilities.

37 new vulnerabilities have been discovered that affect platforms. Customers affected by eCommerce platforms, successfully breached by these vulnerabilities, will be contacted by the relevant companies.

Advice for any online eCommerce businesses using the platform would be to upgrade to the latest patched versions as soon as possible. Security updates should always be applied immediately to help mitigate against vulnerabilities such as these.

By patching the platforms, businesses can help defend against hackers exploiting the flaws which can compromise websites and cause the potential theft of customers' payment card details.

Reports suggest that most of the issues could only be exploited by authenticated users, but one serious flaw was a SQL injection vulnerability which could be exploited by unauthenticated, remote attackers.

If you are running Magento you are advised to patch as soon as possible.

Thank you to NCSC, Kaspersky Labs, Carbon Black and Anomali labs, Recorded Future and McAfee for content.

Stay safe.
Paul