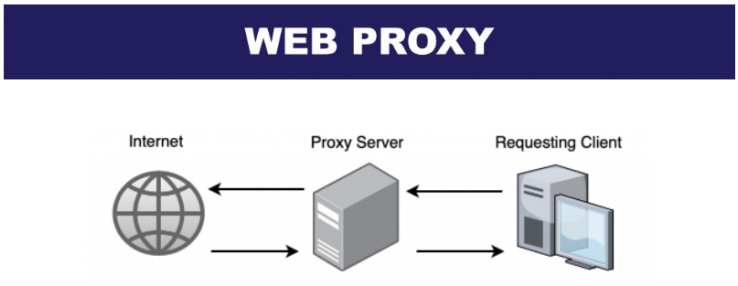
Reactive Measures: Blocking Web-Based Artifacts

Malicious sites pose a huge risk to the employees and need to quickly be neutralized so that even if an employee does click on a link, their request will not be allowed out of the organization's network. We can make malicious sites safe for employees by implementing rules within the web proxy, a device that sits on the perimeter and allows or disallows connections. Think of schools blocking games websites or adult content – that's the web proxy doing its magic. We can also use perimeter firewall blocks to prevent employees from connecting to a malicious IP, but this is usually rare, and a proxy block will be enough to prevent any connections.



There are two types of blocks we want to make on a web proxy – a URL block, and a domain block.

URL Blocks

URL blocks are extremely specific, and will **only** block the URL that has been provided. If we have a credential harvester that is using the URL "hxxp://elephantsanctuary[.]com/index/2019/hgasdf/11/outlook/owa.php?" and we block this on the web proxy, whilst this will block this URL that is being used in the observed emails (this is effective because the URL can't be changed once the emails have been sent), if the attackers send another attack to the same targets with a slightly modified URL that's using the same domain, this block becomes ineffective.

Sometimes URLs are dynamically generated for specific recipients, and therefore a URL block would only neutralize the threat for one recipient. Examples of this include URLs that auto-fill the email address per phishing email (URL will end in "=john.smith@domain.com" or similar).

We can block URLs at a specific point, in order to be more effective and catch more potential malicious URLs. In the example above ("hxxp://elephantsanctuary[.]com/index/2019/hgasdf/11/outlook/owa.php?") we could block the first directory that looks suspicious, in this case, it would be "hgasdf". By blocking "domain[.]com/index2019/hgasdf", anything that comes after that directory will be blocked and the connection will not get outside of the network.

So when deciding on a URL block, work out if the full URL is static and would work for all recipients, or if there is an obviously malicious directory where the URL block can end.

Domain Blocks

Domain blocks work to prevent access to an entire domain. If we wanted to block Google.com (please dear god never do this), then it would prevent any web requests going out to Google, including any subdomains or any URLs. Revisiting the example above, if the domain was discovered to be created with purely malicious intent or has been compromised and there is no business justification for employees to visit the site, we can block the entire domain, in this case, it would be "elephantsanctuary[.]com". This would make any future attacks using the same domain, but

new URLs, ineffective because traffic to that domain is already prohibited, and will never leave the organization.

DNS BLACKHOLING

Whilst firewalls and proxies are the standard method of blocking access from a private network out to resources on the internet, DNS blackholing can be used as a protective measure, but also an educational one. Blackholing is the process of creating a fake DNS entry so that if an employee tries to access "hxxp://thisisreallymalicious.com" they will actually be sent to another site. If an organization is hit by a large-scale campaign, and a high number of employees receive the same phishing email with a URL in it, blocking the domain (if appropriate) could be accompanied with a DNS blackhole, so if users click the link it goes to a safe landing page, telling them they just clicked a malicious URL. SIEM or EDR alerts can also be generated on any users making an outbound connection to the blackholed domain, so they can be highlighted for additional security awareness training.

FIREWALL

When there are multiple malicious sites being hosted on the same IP, if there is no legitimate resource that the business would need access to running on that IP, we can block that server to prevent access to any of the sites on it. This is an extreme measure, and is typically not conducted when regarding phishing, and is often used to block IPs that are scanning or attacking the organization. Under the intelligence concept the 'Pyramid of Pain', which we cover in the Operational Intelligence section of the Threat Intelligence domain, IP addresses are the second easiest indicator for malicious actors to change, so it is likely that IP blocks will be countered by simply using a new IP, rendering the block useless.

MAKING THE DECISION

The first thing you need to consider, has the domain been created for purely malicious activity, or has it been compromised? (We covered this earlier. Use WHOis lookups to see the domain age, use URL2PNG to look at the root domain and see if there is a legitimate site, do Google background checks).

If the domain has been created for purely malicious intent (young age, no legitimate content, malicious content present) then you have sufficient justification to make a domain block on the web proxy. The site is malicious, and employees have no legitimate reason to visit it. It poses a risk to the business – mitigate the risk by blocking it.

If the domain has been compromised then you need to decide **whether employees would ever need to visit this domain for business purposes.** If they don't, then the site can be domain blocked on the web proxy. The site has security weaknesses and has been taken over by hackers. If no employees need to access it, then there will be no negative impact by blocking it.

If the domain has been compromised and **employees may need to visit the site** then you should request a URL block, and ensure that the URL is appropriate for the type of attack observed. Can you block the full URL? Do you need to bring it down a couple of directories to include other malicious pages that the site may hold?

Previous Topic

Mark Complete

Next Topic

Back to Lesson