What is Island Hopping?

More and more, cybercriminals are targeting smaller organizations as a means to attack larger ones. Attackers are exploiting vulnerabilities in the defenses of these less sophisticated companies and using their affiliation with the target as a point of entry. This is known as “Island Hopping”—a term derived from a World War II military strategy of the same name.

According to VMware Carbon Black’s recent Threat Report, half of today’s attacks leverage island hopping. This means organizations need to be hyperaware that attackers are after not only their network, but all those along their supply chain as well. Businesses must ensure that companies they work closely with are doing due diligence around cybersecurity, too.

The goals of these types of attacks can vary, but there has been a steep increase in attempting intellectual property theft—up 17% from last quarter. Financial gain remains the most common objective, representing 61% of island hopping attacks. When asked why their organizations were vulnerable to these attacks, “lack of visibility” was named the top barrier to incident response.
How Does It Work?

As island hopping has grown in prevalence, three forms have emerged as the most common.

1. **NETWORK-BASED “ISLAND HOPPING”**
   
   Network-based island hopping is the most common form of the technique and what is usually referred to by the term. With network-based island hopping, attackers infiltrate one network for the purpose of “hopping” onto an affiliate network. Recently, this has commonly come in the form of attackers targeting an organization’s managed security services provider (MSSP) to move through their network connections.

2. **WEBSITES CONVERTED INTO “WATERING HOLES”**
   
   While much less common, “watering hole” attacks made up a solid portion of island hopping attacks seen in early 2019 (17% according to VMware Carbon Black’s Threat Report). In these attacks, hackers will target a website frequented by partners or customers of the organization they are trying to breach. Most commonly, hackers will inject malware into the target site that will then infect the individuals using the site, providing the attackers with the information or access they need to move onto the next stage of their attack.

3. **REVERSE BUSINESS EMAIL COMPROMISE (BEC)**
   
   Reverse Business Email Compromise represents a newer trend in cyber crime occurring mainly in the financial sector. These attacks are achieved when a hacker successfully takes over a victim’s mail server to wage fileless malware attacks against members of an organization who are prone to trusting what seem to be legitimate emails coming into their inbox.
How VMware Carbon Black Combats Island Hopping

VMware Carbon Black provides best-of-breed endpoint visibility and prevention through our cloud-native endpoint protection platform (EPP), using a single lightweight agent and leveraging a simple, unified interface.

While attackers will most commonly utilize network-based island hopping techniques for initial infiltration, this is not where their work stops. If they are able to successfully hop from a supplier or customer’s network onto your own, they will undoubtedly attempt to wreak havoc on your endpoints, whether that’s through detonating pieces of malware, architecting and deploying a zero-day variant of ransomware, or utilizing different living-off-the-land techniques in an attempt to weaponize known-good software and obfuscate their presence. The VMware Carbon Black Cloud activity,
and analyzes the behaviors associated with that activity in the cloud, to identify and prevent malicious actions—even if they are being propagated by unknown or known-good applications.

Reverse Business Email Compromise (discussed in the section above) is a common step attackers take once they’ve successfully infiltrated a network and gained credentials to an email account. An attacker might then begin sending emails out to the rest of the organization under the trusted domain name, attaching a weaponized Excel document, with instructions to open, that sparks no concern. We cannot expect end users to be 100% vigilant in these situations—especially if there are no logical clues that the situation could be malicious—so the Excel file is opened. After this, the embedded macro begins executing and invoking Powershell scripts that ultimately attempt to encrypt user data files, acting as a zero-day piece of ransomware. VMware Carbon Black would see this entire scenario unfold, tagging every behavior along the way, and apply prevention when those behaviors turn inherently malicious. This data is then strung together and displayed to the administrator in an easy-to-understand process tree—showing exactly how this situation got started, each step along the way, and when VMware Carbon Black applied prevention—allowing for further remediation if necessary. The end user is also able to see real-time alerts associated with their device, enabling them to help close the mean-time to resolution as well.
Reverse Email Business Compromise; a weaponized Excel file launched from Outlook and then began running malicious Powershell scripts, which were prevented by CB Defense.
The malicious Powershell script that was spawned by an Excel macro, prevented from invoking a piece of malware.
TO LEARN MORE AND SEE HOW YOU CAN
COMBAT THREATS IN YOUR ENVIRONMENT, VISIT

CARBONBLACK.COM/EPP-DEMO