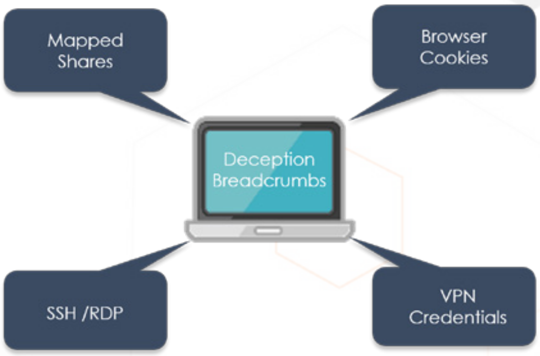
ThreatStrike™ End-Point Deception Suite

The Attivo ThreatStrike Endpoint solution, part of the modular ThreatDefend Platform, provides early and accurate detection of targeted attacks on endpoints and servers. Customizable and non-intrusive, this agentless deception technology places bait and breadcrumbs that lead to an engagement server, where an alert is raised, attacks are analyzed, and actions to quarantine the infected system are activated.



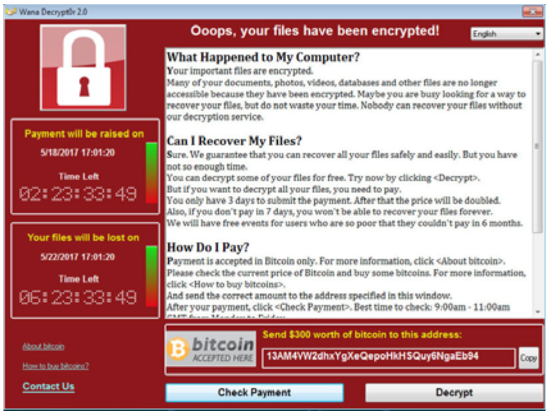
To reach sensitive network data, attackers will compromise computers to steal passwords and hashes that can then be used to move laterally within the network and escalate privileges to advance their attack. The ThreatStrike solution is an agentless technology that dynamically plants deception credentials, lures, and deception network drives for ransomware detection.

Automated Attack Analysis and Forensic Reporting

The Attivo ThreatStrike suite provides real-time attack analysis and alerts on the use of planted deceptions. Once an attacker takes the bait and tries to use the deceptive credentials, they are led to the Attivo BOTsink Solution, which identifies the infected endpoint, analyzes the attack, and provides 3rd party integrations to share information and automate response actions with prevention devices. Additionally, SIEM applications can be queried to check and raise alerts based on the failed login use of deception credentials, providing accurate alerts for notifications that would typically be buried and lost in logs of data. The BOTsink analysis engine also goes one step further than typical sandboxes by capturing and analyzing memory forensics as part of the attack analysis. All too often, this data is lost, and along with it, the attacker's tracks. This unique benefit will often provide the much-needed insight to truly understand and quickly respond to an attack.

Ransomware Solution

Ransomware works by infecting and encrypting attached network shares on a device. The Attivo ThreatStrike endpoint lures, however, combat this process by having SMB shares mapped to the BOTsink decoy engagement VMs. Therefore, when ransomware infects a device that has ThreatStrike SMB lures installed, the ransomware encrypts the mapped decoy network shares in place of the production shares. In testing trials of this technology, it was noted that the Attivo high-interaction deception can slow down the encryption attack cycle by a factor of 25 times, keeping the ransomware busy encrypting a continuous feed of deception files. Analysis of Petya/NotPetya and WannaCry attacks by Attivo Labs demonstrate the effectiveness of deception technology in detecting and stopping ransomware attacks.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/18/2017 17:01:20
Time Left
02:23:33:49

Your files will be lost on
5/22/2017 17:01:20
Time Left
06:23:33:49

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Phishing (often the weak link) Detection

As part of the endpoint suite, the solution provides additional protection for what is often the weakest link in the organization, the employees, who continue to fall for and activate phishing emails. The ThreatStrike suite provides an email submission plug-in for suspicious email submission, automated analysis (through the BOTsink analysis engine), and summary reporting to determine the malicious nature of emails. Companies will benefit by providing a simplified way for employees to submit suspicious emails and from the automation of analysis, which can save hours of tedious email review and reporting.

Conclusion

It is critical to detect the attacker the moment they penetrate the network. The ThreatStrike Endpoint Deception Suite provides the crucial detection of credential based attacks that are inherently missed with anti-virus and other forms of perimeter defense. Regardless of the attack vector an attacker is using to breach a network, the Attivo ThreatDefend Platform provides a comprehensive offering of network, endpoint, data, and application deceptions to efficiently and accurately reveal attacker presence, analyze the attack, and simplify incident response.

About Attivo Networks

Attivo Networks® is the leader in dynamic deception technology for real-time detection, analysis, and accelerated response to advanced, credential, insider, and ransomware cyber-attacks. The ThreatDefend Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments. www.attivonetworks.com