CYBERSEER

MANAGED SECURITY SERVICE (MSSP) FOR THREAT DETECTION & ANALYSIS

Cyber threats are increasing daily in both number and sophistication. As a business's intelligence grows, so does its critical data. Business relies on the confidentiality, integrity and availability of its data. Having visibility in the core of your network is vital to detect the presence of sophisticated threat actors. Identifying these threats early in their life-cycle allows an organisation to respond quickly and effectively.

Cyberseer operates a portfolio of advanced threat technologies under our threat detection and analysis service. This is an intelligence driven service leveraging expert human analysis to provide timely, accurate and actionable information about the threats we have identified in your environment.

Our Analysts operate within a mature alert handling process to harness the intelligence from our deployed technologies. Cyberseer alerts you to new threats as they occur and provides you with regular detailed reports on the current threat status in your environment.

ADVANCED THREAT ANALYSIS:

Our Analysts are highly trained in configuration and optimisation of the Cyberseer advanced threat detection technologies which provide the foundation for their analysis capabilities. Analysts continually review the output from deployed technologies to identify unusual or concerning patterns of behaviour that may be indicative of threats.

Once identified, threats are investigated within the Cyberseer incident analysis framework which aims to balance the competing goals of comprehensive analysis and time-critical response. This framework is based around a scoring and escalation process designed to provide the information you need to prioritise and effectively respond to threats. Rather than compiling a long list of alerts or Indicators of Compromise (IOC's), our Analysts draw on their experience, the context of the alert in your environment and external sources of intelligence to provide you with an explanation and analysis of each threat they discover.

When deciding how to respond to possible threats within your environment, it is useful to ask yourself two questions:

- **How good is the evidence for this threat?**
- **How serious would the consequences be if it was real?**

To aid this decision-making process our Analysts rate each threat by both severity and confidence, so you can effectively decide what to prioritise. These separate scores are combined to give you a sense of the urgency of each threat, with the most urgent ones communicated to you upon discovery.

24/7 SERVICE:

Cyberseer's customer operate both globally and flexibly in an always on environment, as do their adversaries, pushing the need for an always on service. Cyberseer delivers an affordable 24/7 priority threat reporting option, without increasing your organisations' staff overhead costs.

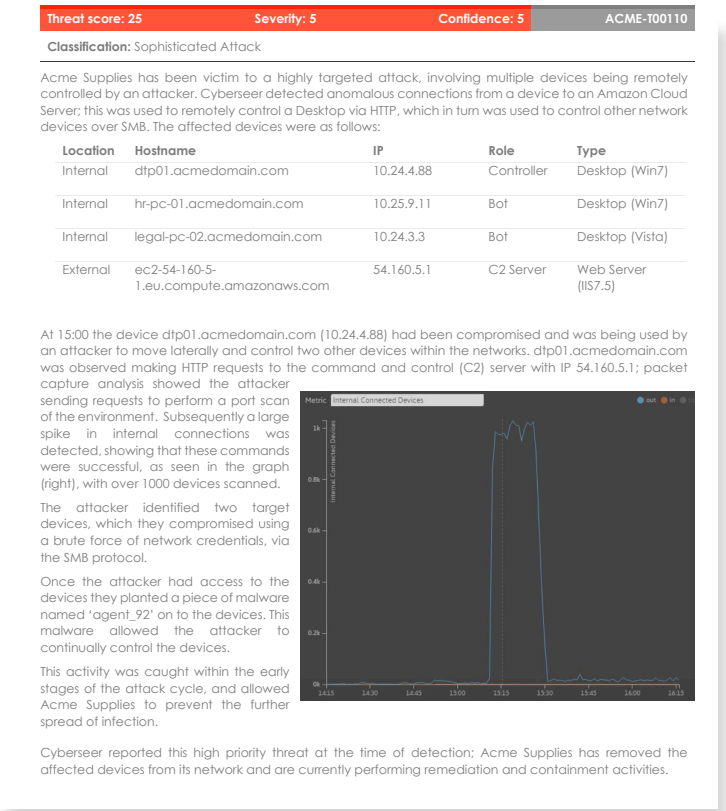
Our Forensic Analysts become an extension of your internal team; Cyberseer triage an event that breaches the priority thresholds, and, should a severe threat be detected, the Cyberseer team will notify a contact defined in the escalation process with incident details, forensic analysis and recommended remediation for incident response. This not only helps to protect your organisation from a breach but also saves valuable time for your IT Security team.

REPORTS:

As well as communicating priority threats as they are discovered, our Analysts track and record the details of each threat investigated. The scores and classifications of less urgent threats are used to produce monthly Threat Intelligence Reports. The core of these reports is the Threat Rating, as illustrated in the charts below which provides a relative measure of the number and seriousness of identified threats in your network.

The bar chart below illustrates how the Cyberseer service tracks and trends this rating on a month by month basis, so you can see whether your threat status is improving. The monthly reports break down this threat score by threat categories, enabling you to identify areas of weakness in your security posture and make informed investment decisions to bolster your defence in depth.

Each report includes technical details on identified threats as well as an executive summary, so you can quickly gauge the nature and seriousness of the threats you are currently facing.



Threat score: 25 | **Severity: 5** | **Confidence: 5** | **ACME-T00110**

Classification: Sophisticated Attack

Acme Supplies has been victim to a highly targeted attack, involving multiple devices being remotely controlled by an attacker. Cyberseer detected anomalous connections from a device to an Amazon Cloud Server; this was used to remotely control a Desktop via HTTP, which in turn was used to control other network devices over SMB. The affected devices were as follows:

Location	Hostname	IP	Role	Type
Internal	dtp01.acmedomain.com	10.24.4.88	Controller	Desktop (Win7)
Internal	hr-pc-01.acmedomain.com	10.25.9.11	Bot	Desktop (Win7)
Internal	legal-pc-02.acmedomain.com	10.24.3.3	Bot	Desktop (Vista)
External	ec2-54-160-5-1.eu.compute.amazonaws.com	54.160.5.1	C2 Server	Web Server (IIS7.5)

At 15:00 the device dtp01.acmedomain.com (10.24.4.88) had been compromised and was being used by an attacker to move laterally and control two other devices within the networks. dtp01.acmedomain.com was observed making HTTP requests to the command and control (C2) server with IP 54.160.5.1; packet capture analysis showed the attacker sending requests to perform a port scan of the environment. Subsequently a large spike in internal connections was detected, showing that these commands were successful, as seen in the graph (right), with over 1000 devices scanned.

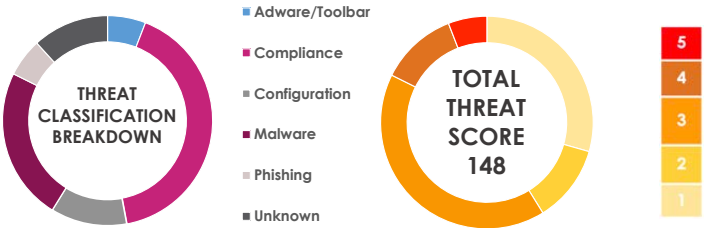
The attacker identified two target devices, which they compromised using a brute force of network credentials, via the SMB protocol.

Once the attacker had access to the devices they planted a piece of malware named 'agent_92' on to the devices. This malware allowed the attacker to continually control the devices.

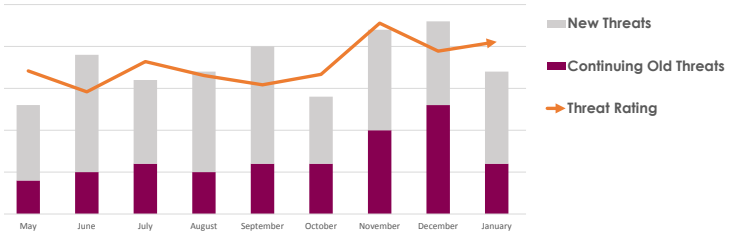
This activity was caught within the early stages of the attack cycle, and allowed Acme Supplies to prevent the further spread of infection.

Cyberseer reported this high priority threat at the time of detection; Acme Supplies has removed the affected devices from its network and are currently performing remediation and containment activities.

Extract from a sample Cyberseer Threat Intelligence Report



Threat Classification and Rating Charts extracted from a sample monthly Threat Intelligence Report.



Monthly Threat Trending Chart extracted from a sample Threat Intelligence Report.

SERVICE SUMMARY:

Cyberseer provide advanced threat detection services to global enterprise organisations across a wide range of market verticals in North America, Asia, Europe and Australia. Organisations leverage these services and contribute to the 170,000 devices which Cyberseer has visibility of daily.

By combining market leading machine learning technology with the human intelligence of Cyberseer's Forensic Security Analysts, we can deliver the following services:

- **Pro-active detection of unknown**, advanced insider threats.
- **Threat identification and classification** by experienced cyber security analysts.
- **Priority and detailed actionable alerts** for serious threats requiring urgent action at time of discovery.
- **Support** for client's threat investigations.
- **Detailed threat intelligence reports.**
- **Quarterly service meetings** to review the service and ensure our client's expectations are being met.

CYBERSEER

CONTACT US

+44 (0)203 823 9030
info@cyberseer.net
www.cyberseer.net