GOOSE VPN - Cyber Alarm – Categories

Threat level	Enabled	Name	Description
Various	✔	Blacklisted hostnames and URLs	Connections to blacklisted hosts, detected by means of hostnames instead of IP addresses. This provides a means for detecting connections to malware in shared hosting environments, for example.
1	✔	Botnet Controller	Infected clients in your network will periodically connect to the Botnet Controller (or Command and Control server) to maintain contact with the attacker. This connection is facilitated using any available protocol to connect to any IP-address used by the attacker. Most controllers use port 80 and port 443 to obscure the data's digital footprint. This method enables malware to bypass your firewall by making it look like ordinary web traffic. An alert in this category should be investigated at all times.
	✔	Malware-specific behavioral heuristics	Heuristics that are based on network-based characteristics of specific malware families, such as HTTP request structures, specific user agents and others.
	✔	Sinkhole	Malware is active on your client's system, but the controller IP has been seized or diverted in order to disable the botnet. The infected client still tries to connect to it and, therefore, a breach and an infection occurred in the past.
	✔	Tor Network	The Tor Network is designed to offer anonymous Internet access to its users and can also be used to hide a Botnet Controller. Anonymous access could be a used as a means to subvert company usage policy or even engage in illicit activity. Since mid-2013, the Tor Network has been used by an increasing number of operators to hide communications with Botnet Controllers. If not initiated by an employee, then an infection is present within your network. An alert in this category should be investigated at all times.
2	✔	Disguised executable file	Downloads/uploads of disguised executable (.exe) files. This type of file is often used as payload to mislead users.
	✔	Experimental	This collection of heuristics is experimental and may require further investigation.
	✔	Mining Pool	Cryptocurrencies are generated by users who offer their CPU or GPU power to calculate complex algorithms. The calculating power is rewarded with cryptocoins which can be exchanged for cash. A mining pool occurs when multiple people combine computing resources to produce cryptocurrencies. Malware writers are always looking for ways to make money and illicitly using your computer to generate cryptocurrencies pays off. In addition to malware, mining can also be done by personnel who uses resources for personal benefit. An alert in this category should warrant further investigation.
	✔	Miscellaneous	New methods used by cyber criminals appear daily. When we see a threat that does not fit any other category, it will be placed into the Miscellaneous category. When a specific method recurs over a longer period, it will be moved to a new dedicated category. It is advised that you review the meta-data of the alert, as it can provide some insight into the nature of the threat.
	✔	Path traversal	Indicators of path traversal in URLs. This may signal attempts to access confidential files elsewhere in the directory structure, such as password files. This technique is often used as a starting point for hacking.
	✔	Periodic heartbeat	Periodic heartbeat connections, indicating potential malware infections. Heartbeats are behavioral characteristics of botnets and other malware types.
	✔	Port scan	Identifies both horizontal and vertical network port scans. Horizontal port scans are scans against a specific port on different hosts. Vertical port scans are scans against different ports, on the same host.
	✔	Web shells	Indicators of potentially malicious shell placed on a Web server by malicious actors. Used to add, modify or remove data on the compromised server.
3	✔	Adware	Connections towards Adware / PUP networks. This module reports on adware and potentially unwanted program (PUP) connections. Adware and PUPs are designed to serve advertisements, and may redirect your search requests to advertisement Web sites that collect marketing data about you.
	✔	Bad Internet Neighbourhood	Cyber criminals have a preference for Internet Service Providers that offer services without asking their customers too many questions (e.g., few rules, anonymous payment methods, etc.). These IP-addresses are frequently used in targeted attacks, phishing/pharming campaigns or as Botnet Controllers.
	✔	BitTorrent tracker	Connections towards BitTorrent trackers based on URL structure. A BitTorrent tracker is a server that connects peers using the BitTorrent protocol.
	✔	Cloud Storage Service	Certain cloud services are considered more harmful than others based on their user policy.
	✔	File sharing	Connections towards Peer-to-peer (P2P) networks. This category includes connection patterns for various P2P networks.
	✔	Filesharing Tool	Filesharing tools, such as eMule and Bittorrent, are used to download music, movies and software from other users in that network. Most of these protocols are illegal to use due to the sharing of copyright-protected material. About 60% of the software found in the most popular P2P networks has malware attached to it; unfortunately, users are typically unaware of this risk. Even the software used for sharing files may present a risk, as they are frequently not secure. The sharing of unwanted directories is also common.
	✔	Instant Messaging	Well known and less known IRC-servers are occasionally used in malware campains.
	✔	Instant messaging	Connections by instant messaging (IM) applications.
	✔	Public Proxy	A computer user can use a public proxy to re-route their browser through a different system. This is frequently done to bypass URL-based company policies. In addition, malware can also use public proxies to spread infections. An alert in this category should warrant further investigation.
	✔	Remote Administration	Remote administration tools / desktop sharing tools can be used with good intent, but can also be used to dangerous effect by malware and consequently used in social engineering attacks. Well-intended actions, such as remote working programmes, are often facilitated via remote administration tools but doing so opens up a gap in your security environment. Certain tools, regardless of popularity, can be detected based on 3rd party IP-addresses; others can be detected via their port number. TeamViewer, for example, can be detected even though no connection is in-place.
4	✔	Geofence	In an open network, connections to these countries will occur regularly; secure networks, however, should limit accessibility to IP-addresses from questionable locations. Browsing less popular websites, international NTP-pools (time servers) and P2P software will trigger an alert for this category. In maximum security networks, connections to IP-addresses from this category require attention.
			✔ Syrian Arab Republic
			✔ Iran, Islamic Republic of
			✔ Nigeria
			✔ Indonesia
5	✔	Domain Parker	Domain parkers are IP's which host expired domains. Recurring connections to domain parkers can indicate infection with malware.
	✔	Dynamic DNS domains	HTTP requests towards dynamic DNS domains. Persistent connections towards dynamic DNS domains may indicate infections by various backdoors and trojans.
	✔	Free hosting domains	Connections towards free hosting domains. These environments are often used by threat actors to perform attacks, such as phishing, or to exfiltrate stolen data towards the hosting environment.
	✔	IP Self Check Service	IP Self-Check services are web-based services which show the extern (public) IP of the source host. These services are extensively used by malware and recurring connections to IP Self Check Services can indicate indection with malware.