FireEye
SECURITY REIMAGINED

CYBER THREATS TO THE RETAIL AND CONSUMER GOODS INDUSTRY

SECURITY
REIMAGINED

Retail and consumer goods companies face cyber threats from the following actors:

- Enterprise-like cybercriminals seeking to obtain financial account and other customer data that they can monetize. These threat actors may target point-of-sale (PoS) systems, or customer databases to harvest user credentials, stored financial data, stored personally identifiable information (PII), and similar datasets.
- Advanced Persistent Threat (APT)[1] actors aiming to support their domestic businesses by providing them with innovative technology or a competitive edge over their competition. These threat actors may seek to understand supply chains, manufacturing processes, and programmatic business details to replicate these processes or identify weaknesses.

OBSERVED TARGETING

We have observed at least 8 advanced threat groups compromise companies in these subsectors

Subsectors Compromised

Consumer Products Manufacturing	In-store Retail
Consumer Services	Online/Non-store Retail
Food & Beverage	

Data Stolen from Retail & Consumer Goods Companies

Credit Card Track Data	Personal Identification Numbers
Customer Names, Account Information, & Credentials	Other Financial Data
Primary Account Numbers	

[1] Advanced Persistent Threat (APT) actors are assessed to take direction from a nation state to steal information or conduct network attacks, tenaciously pursue their objectives, and are capable of using a range of tools and tactics.

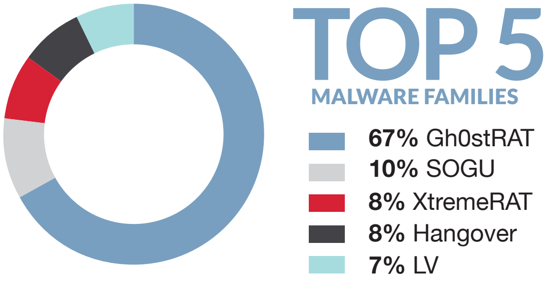
CASE STUDY: MULTIPLE THREAT GROUPS COMPROMISE RETAILER'S NETWORK, ACCESS CUSTOMER ACCOUNTS

Employees at a retail company discovered that the company's network had been compromised when customers began reporting that the online ordering system was functioning poorly. When investigating the company's network traffic, we found that at least three separate advanced threat groups had compromised the company and executed a high number of unauthorized transactions - hence the degraded performance.
The threat actors appeared to have gained access to all customer accounts and associated credentials. Altogether, the threat groups accessed sensitive pricing information for nearly 500 customers.

THREAT HORIZON AND INDUSTRY OUTLOOK

Companies in the retail and consumer goods industry will likely continue facing cyber security risks from both cybercriminals and APT groups working in association with a nation state government. The following factors may influence future targeting in the sector:

- Cybercriminals may take advantage of busy holiday shopping seasons to compromise retailer payment systems and steal customer information at a time when the high volume of activity may help hide malicious network activity.
- Companies that develop new and cutting-edge products may experience additional targeting from APT groups seeking to obtain proprietary product information that would provide indigenous companies with a competitive market advantage.
- We consider that cybercriminals may increasingly target the retail sector where companies adopt new payment systems, seeking to take advantage of any previously undetected vulnerabilities or security flaws in these systems.
- APT groups may also target foreign companies that are entering into trade negotiations with their sponsoring government or indigenous companies. By stealing internal communications, business information, or other proprietary information, the threat group might provide its sponsoring government, or state-owned companies, with an insider advantage in the negotiations, helping to secure advantageous terms.



FireEye most frequently detected threat actors using the following targeted malware families to compromise organizations in the retail and consumer goods industry:

Gh0stRAT

is a remote access tool (RAT) derived from publicly available source code. It can perform screen and audio captures, enable a webcam, list and kill processes, open a command shell, wipe event logs, and create, manipulate, delete, launch, and transfer files.

SOGU

(aka Kaba aka PlugX) is a backdoor capable of file upload and download, arbitrary process execution, filesystem and registry access, service configuration access, remote shell access, and implementing a custom VNC/RDP-like protocol to provide the command and control (C2) server with graphical access to the desktop. It provides SQL database-querying capabilities and may communicate using HTTP POSTs or a custom binary protocol.

XtremeRAT

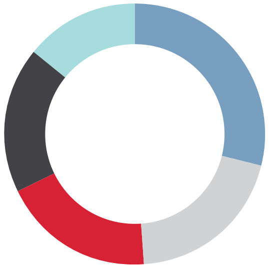
is a publicly available RAT capable of uploading and downloading files, interacting with the Windows registry, manipulating processes and services, and capturing data such as audio and video.

Hangover

refers to multiple malware families used during Operation Hangover threat activity originating from India. These malware families are capable of keylogging, backdoor functionality, and information stealing, and could be used during a variety of intrusion phases. The families share common command and control infrastructure.

LV

(aka NJRAT) is a publicly available RAT capable of keystroke logging, credential harvesting, reverse shell access, file uploads and downloads, and file and registry modifications.
It also offers threat actors a "builder" feature to create new variants.



TOP 5

CRIMEWARE FAMILIES

- 🟦 **29%** H-WORM
- ⬜ **20%** ASPROX
- 🟥 **19%** PALEVO
- ⬛ **18%** KOREDOS
- 🟦 **14%** ZEUS

FireEye's sinkhole and dynamically shared threat data indicate that the following crimeware variants were the most commonly detected in the retail and consumer goods industry

H-WORM

is a Visual Basic Script - based RAT that has been used in targeted attacks as well as in a wider context as attacks through spammed email attachments and malicious links.

ASPROX

is a spam botnet that typically uses themes related to airline tickets, postal services, and license keys in order to entice victims to open the emails and download malicious software.

PALEVO

is an information-stealing worm that spreads over removable drives, network shares, P2P, and instant messenger programs. Infected machines communicate with C2 over UDP port 53.

KOREDOS

is a trojan that can encrypt user files, destroy the master boot record, and force infected systems to participate in distributed denial of service attacks.

ZEUS

(aka Zbot) is a family of Trojans primarily designed to engage in banking credential theft. It is capable of a wide variety of function, including the ability to remotely execute shell commands.

TOP

MALWARE IN IR"S

The malware families that APT groups most frequently used in incidents that we responded to in this sector include:

ZERODUE

is a backdoor designed to retrieve a Web page from a pre-determined C2 server that it expects to contain special HTML tags. It will attempt to interpret the data between these tags as commands. It is primarily a downloader.

TINROOF

is a dropper that is a set of packed device drivers that target the Windows XP operating system. Once unpacked, the dropper injects shellcode into user space processes and executes the shellcode. Injected shellcode functionality includes key logging, function hooking, stealing credit card data from POS applications, and backdoor functionality.

NEWSREELS

is a HTTP backdoor capable of sleeping for a specified time period, creating processes, providing threat actors with an interactive command shell, and uploading files.

GRABNEW

is a credential stealing backdoor. When loaded within a web browser, it installs API hooks that allow it to monitor network data to harvest user credentials and HTTP form data. It can also extract user certificates and cookies stored on disk, upload and download data, execute arbitrary programs, and implement a modified SOCKS5 proxy.