ScanPOS, new POS malware being distributed by Kronos »

By Nick Hoffman, Jeremy Humble, & Mitch Gonthier

Archived: 2026-04-05 20:41:09 UTC

Just in time for the holidays, a brand new Point Of Sale (POS) malware family has been discovered.

Morphick responded to a Kronos phishing campaign that involved a document with a malicious macro that downloaded the Kronos banking malware. When running, the Kronos payload will download several other pieces of malware, but the one that caught our eye is a new credit card dumper with very low detection. Morphick is tracking this malware under the name ScanPOS due to the build string present in the malware.

```
C:Usersexampledocumentsvisual studio 2010Projectsscan3Releasescan3.pdb
```

At the time of this writing, ScanPOS only scored 1/55 on Virustotal:

ScanPOS, while not extraordinarily impressive or unique, is a new family. It performs the same basic tasks that all other POS malware performs, yet sneaks by almost every developed detection technique. ScanPOS does little in terms of evading detection, which can help it blend in a production environment. When code is heavily packed, it will often get picked up by generic heuristics.

Phish:

The Kronos phish that was delivering the malware was a very basic email with the following body:

```
An Employee has just been terminated.
Name: Tanner Williamson
Employee profile: EmployeeID-6283.doc
Emplid: 2965385
Rcd#: 0
Termination Date: 11/17/2016
```

Relevant headers are below:

```
TIME-STAMP: "16-11-14_13.44.23"
CONTENT-DISPOSITION: "attachment; filename='EmployeeID-6283.doc'"
X-VIRUS-SCANNED: "Debian amavisd-new at hosting5.skyinet.pl"
Subject : An Employee has just been terminated.
From: HR <johns.brueggemann@banctec.com>
Mail-From: web1@hosting5.skyinet.pl
1st rec: hosting23.skyinet.pl
2nd rec:hosting23.skyinet.pl
```

When enabling the macro on EmployeID-6283.doc, the macro will download

```
profile.excel-sharepoint[.]com/doc/office.exe
```

(Kronos Payload) and execute it. Kronos will then download and execute ScanPOS from

```
http://networkupdate[.]online/kbps/upload/a8b05325.exe.
```

Credit Card Dumping:

On execution, the malware will grab information about the current process and get the user (calling GetUserNameA). Privileges are checked to ensure that the malware has the ability to peek into other processes' memory space by checking for SeDebugPrivilege (see below).

The malware will then enter an infinite loop, padded with sleeps, to dump process memory on the box to search for credit card track data. During this loop, the malware iterates processes using Process32FirstW/Process32Next from a process list obtained via CreateToolhelp32Snapshot.

The iterator obtains a handle to the process by using OpenProcess, which is then checked against a basic whitelist, to avoid unnecessary system processes:

If the name of the process passes a check against the whitelist, the malware will continue to get process memory information by calling VirtualQueryEx and then eventually fall to ReadProcessMemory.

Once process memory is obtained, the scanning for credit card track data can begin. The main logic behind this is in function 0x4026C0.

The logic starts with basic sentinel checks and a starting number of 3,4,5 or 6.

The malware will use a custom search routine (rather than regex) to find potential numbers.

After the malware does several checks for credit card information, it will pass the potential candidate to Luhn's algorithm for basic validation.

When it finds a potential candidate that passes Luhn's, it will continue searching for numbers (anything between 0 and 9) until it hits a "?" marking the end of the track data.

Network Connectivity:

Once the potential card numbers are found, the information is sent via HTTP POST to invoicesharepoint[.]com.

Summary:

ScanPOS is being distributed through an active campaign. With only 1 anti-virus engine flagging this executable as malicious, this family helps show the constant pressure that AV vendors face while trying to stay ahead of the

curve. Being distributed in a macro is a simple technique that has been covered in detail in many different blog posts and may have helped this family hide a little bit in the noise.

Indicators of Compromise:

Indicator	Type	Notes
invoicesharepoint.com	Domain	ScanPOS C2 & data dump (46.45.171.174)
/gateway.php	URI	ScanPOS C2 POST uri
networkupdate.online	Domain	Office.exe (Kronos) Downloads additional EXE (46.45.171.174)
www.networkupdate.club	Domain	Office.exe (Kronos) C2 (46.45.171.174)
profile.excel-sharepoint.com	Domain	Dropper DL site from phish (211.110.17.192)
939fcb17ebb3aa7dd57d62d36b442778	MD5	Phish doc: EmployeeID-6283.doc
11180b265b010fbfa05c08681261ac57	MD5	Office.exe (Kronos)
6fcc13563aad936c7d0f3165351cb453	MD5	POS malware: (Kronos DL) a8b05325.exe
73871970ccf1b551a29f255605d05f61	MD5	(Kronos DL) 1f80ff71.exe

f99d1571ce9be023cc897522f82ec6cc	MD5	(Kronos DL) c1c06f7d.exe
/kbps/connect.php	URI	Kronos C2 traffic
/kbps/connect.php?a=1	URI	Kronos C2 traffic
/kbps/upload/c1c06f7d.exe	URI	Kronos Trj DL [a-z0-9],{8}.exe
johns.brueggemann@banctec.com	email	From address
web1@hosting5.skyinet.pl	email	Mail-From address
ftp.itmy520.com	Domain	Found in 73871970ccf1b551a29f255605d05f61

Further Reading

Our colleagues at Proofpoint offer additional technical analysis outlining how Kronos acted as a loader of the ScanPOS malware as the secondary payload.
