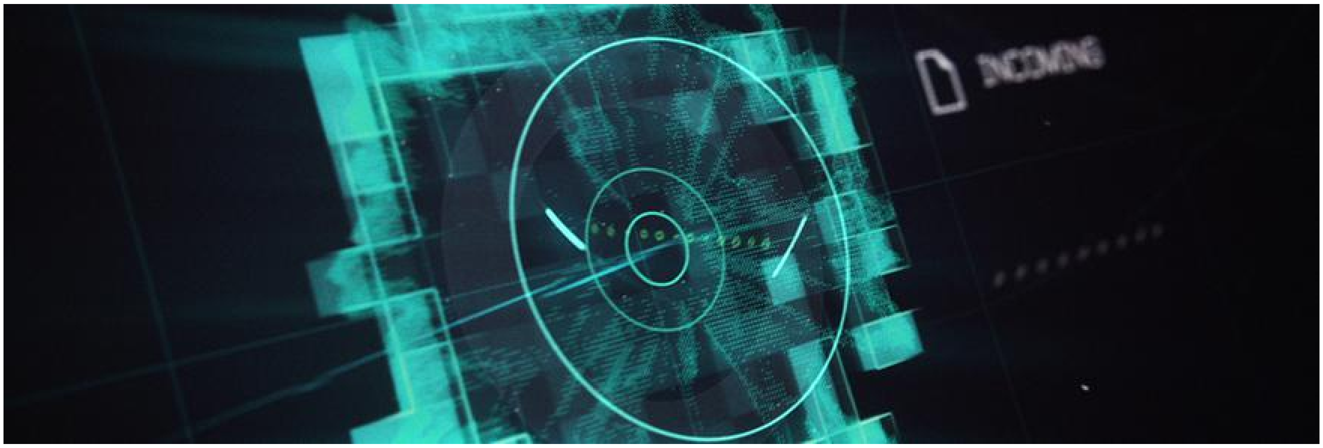
Threat Spotlight: LockPOS Point of Sale Malware

cylance.com/en_us/blog/threat-spotlight-lockpos-point-of-sale-malware.html

The BlackBerry Cylance Threat Research Team



RESEARCH & INTELLIGENCE / 01.16.18 / The BlackBerry Cylance Threat Research Team

LockPOS is a point-of-sale malware discovered in 2017 that is used to exfiltrate payment card data from targeted point-of-sale systems' memory. The most recent version of LockPOS examined here changed its injection technique to drop the malware directly to the kernel to evade detection and bypass traditional antivirus (AV) hooks.

This evasion technique has been seen before being employed by a similar malware (Flokibot POS Malware). In addition to the injection technique, this new malware variant is also communicating with a new command-and-control (C2) server that hasn't been seen before.

The following a technical overview of this new technique used by LockPOS:

File Information

SHA256:1436577b2b111fe299a1321e00543d0e8d49d827abde651faea7403e4bb38644
Type: Win32 EXE
Size: 140,288 bytes
Timestamp: 11/18/2017 12:40:26 PM
ITW names: 1e490056bdb537f9492bc72a365537f0.virobj
1e490056bdb537f9492bc72a365537f0

Technical Analysis

The malware has a core resource section that is encrypted:

Figure 1

When it runs, it begins making API calls that are used to decrypt itself, and the APIs are obfuscated using API hashing:

Figure 2

The decrypted executable with a debugging string shown below is then loaded to memory for execution:

Figure 3

When executed, the malware uses API calls from *ntdll.dll* to inject itself into *explorer.exe* as a persistence mechanism. The API calls are still made using the API hashing, a method that is new for LockPOS which allows the malware to avoid traditional AV detection by injecting the code on-the-fly within memory:

Figure 4

The injected code will then try to connect to the C2 server at the following address:

bbbclearner[dot]at/_x/update[dot]php

This is a new C2 server that has never been seen in malware campaigns prior. The C2 server also has what seems to be a back-end panel that is similar to the one seen before with the *treasurehunter[dot]at* C2 server.

Figure 5

In addition to the abovementioned C2 server, the malware also reaches out to multiple, unregistered domains, most likely as a method used to disrupt any analysis of the file and to hide the real C2 server domain (*a full list of the domains can be found in IOCs section below*).

Figure 6: String in memory showing domains

If you use our endpoint protection product, CylancePROTECT®, you are already protected from this attack.

Indicators of Compromise (IOCs)

Hashes:
1436577b2b111fe299a1321e00543d0e8d49d827abde651faea7403e4bb38644

C2:
bbbclearner[dot]at/_x/update[dot]php

Domains:
reportpestgallon[dot]xyz
siamesefineknowledge[dot]xyz
forkveilfall[dot]xyz
grillpromotionpressure[dot]xyz
grandmothernoveloffer[dot]xyz
shampoodebtorguitar[dot]xyz
commissionroadwaygirdle[dot]xyz
apologytailorpelican[dot]xyz
costsfelonybumper[dot]xyz
marketgreat-grandfatherkettle[dot]xyz
debtdoubleshop[dot]xyz
orderareateaching[dot]xyz
companyresponsibilityshallot[dot]xyz
equipmentkicksaturday[dot]xyz
hyenadecisionblanket[dot]xyz
costscousinphysician[dot]xyz
alibitowerrepairs[dot]xyz
grassarmchairpreparation[dot]xyz
heattomatooffer[dot]xyz
timenoodlesuggestion[dot]xyz
budgethardcoverliver[dot]xyz
productglidinglynx[dot]xyz
objectiveswordfishorchid[dot]xyz
instructionsaluminiumroad[dot]xyz
descriptionbulldozerroast[dot]xyz
authorizationsharonneck[dot]xyz
differencejuicetaste[dot]xyz
myanmarhoodsignature[dot]xyz
inchpaymentvision[dot]xyz

powdergoalship[dot]xyz
koreankeycomparison[dot]xyz
permissionrhythmemery[dot]xyz
smokepigeonpromotion[dot]xyz
budgetpaultrail[dot]xyz
ptarmiganstockbottle[dot]xyz
collarlimitbugle[dot]xyz
employerbatvietnam[dot]xyz
departmentmessagewasp[dot]xyz
ruthbudgetnetwork[dot]xyz
shelfturnoverradish[dot]xyz
copyretailerclose[dot]xyz
massforestopinion[dot]xyz
geminikendocomparison[dot]xyz
billburglartablecloth[dot]xyz
deliverystaircaseangle[dot]xyz
dayfatheropinion[dot]xyz
billwaterfallsoda[dot]xyz
germanquotationconfirmation[dot]xyz
anteaterimprovementgermany[dot]xyz
libraplasticapology[dot]xyz
possibilityneedjennifer[dot]xyz
decisionsnowmancod[dot]xyz
handlegumsalary[dot]xyz
tuneavenuecomparison[dot]xyz
donkeybillmexico[dot]xyz
whipdifferencerecess[dot]xyz
pancreasreportsnake[dot]xyz
pricemedicinejump[dot]xyz
bombapologystreetcar[dot]xyz
departmentrussianfall[dot]xyz
amountdebtorromania[dot]xyz
increasestationcollar[dot]xyz
nickelreportaccountant[dot]xyz
confirmationhaircutpsychology[dot]xyz
outputvacuumproperty[dot]xyz
armyindustrymail[dot]xyz
smilejacketemployer[dot]xyz
schooljapanesecustomer[dot]xyz
ikebanadiscussionapology[dot]xyz
danielheightreduction[dot]xyz
growthpumpyacht[dot]xyz

cocktailtransportexistence[dot]xyz
pricedogsquash[dot]xyz
alloyimprovementterritory[dot]xyz
badgecupdifference[dot]xyz
estimatemimosalan[dot]xyz
summermosquemistake[dot]xyz
illegalauthorizationcourt[dot]xyz
nutobjectiveinvention[dot]xyz
supportfaceoperation[dot]xyz
paymentfilewave[dot]xyz
advertiseindonesiahot[dot]xyz
permissionhandmosque[dot]xyz
competitionweaponjail[dot]xyz
colonyarchaeologyinstructions[dot]xyz
salespressurelock[dot]xyz
selfdeliverynail[dot]xyz
opinionpurchasebathroom[dot]xyz
statisticcreekprofit[dot]xyz
guaranteelistmichael[dot]xyz
competitioncrabquotation[dot]xyz
israelseashoregoods[dot]xyz
coverapologyfeedback[dot]xyz
perchinterestdowntown[dot]xyz
archeologysister-in-lawmarket[dot]xyz
indexemployeecheese[dot]xyz
chequeordersale[dot]xyz
competitionstocksister[dot]xyz
bucketbudgetplot[dot]xyz
retailerperiodicalsponge[dot]xyz

References:
https://www.darkreading.com/endpoint/lockpos-malware-sneaks-onto-kernel-via-new-injection-technique/d/d-id/1330757

The BlackBerry Cylance Threat Research Team

About The BlackBerry Cylance Threat Research Team

The BlackBerry Cylance Threat Research team examines malware and suspected malware to better identify its abilities, function and attack vectors. Threat Research is on the frontline of information security and often deeply examines malicious software, which puts us in a unique position to discuss never-seen-before threats.

Back