# Weiterentwicklung anspruchsvoller Spyware: von Agent.BTZ zu ComRAT

blog.gdata.de/2015/01/23779-weiterentwicklung-anspruchsvoller-spyware-von-agent-btz-zu-comrat

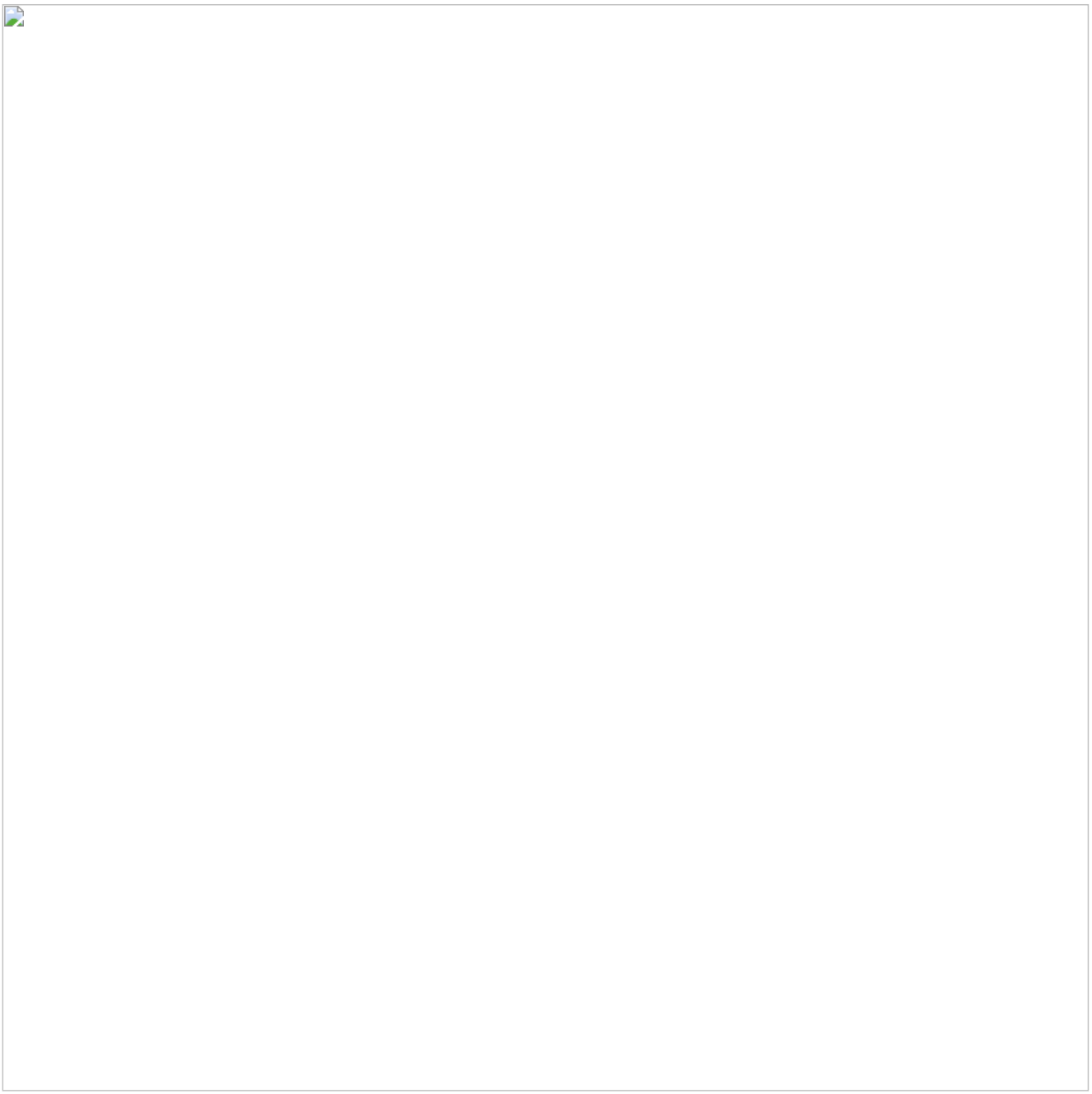
Im November 2014 veröffentlichten die Experten der G DATA SecurityLabs einen Artikel über ComRAT, den Nachfolger von Agent.BTZ. Wie wir damals erläuterten, stand dieser Fall mit dem Uroburos-Rootkit in Verbindung. Wir gehen davon aus, dass der Entwickler, der hinter diesen Kampagnen steht, verschiedene Malware-Stämme nutzt, um die anzugreifende Infrastruktur zu kompromittieren: Uroburos, ein Rootkit; Agent.BTZ/ComRAT, Fernsteuerungstool oder Linux-Malware und vielleicht sogar noch mehr.

Wir entschlossen uns dazu, Agent.BTZ und ComRAT noch einmal genauer unter die Lupe zu nehmen. Deshalb haben wir die Entwicklung dieses Fernsteuerungstools über sieben Jahre untersucht. Die folgende Tabelle enthält minimale Informationen über 46 verschiedene Samples:

| MD5\|Version\|Compilation Date |
|---|
| b41fbdd02e4d54b4bc28eda99a8c1502\|Ch 1.0\|Wed Jun 13 07:31:32 2007 UTC |
| 93827a6c77e84ffdd9c793d485d3df6e\|Ch 1.0\|Wed Jun 13 07:31:32 2007 UTC |
| 3e9c7ef54ea3d55d5b53abab4c3e2385\|Ch 1.0\|Wed Jun 13 07:31:32 2007 UTC |
| b9ed8876ef5a05ba364a9cdbdf4f184d\|Ch 1.0\|Tue Jun 19 12:41:21 2007 UTC |
| d8f98f64687b05a62c81ce9e52dd808d\|Ch 1.1\|Tue Jun 26 08:46:11 2007 UTC |
| 2cf64ff9dad8d64ee9322e390d4f7283\|Ch 1.1\|Tue Jun 26 08:46:11 2007 UTC |
| 24e679155697bd31b34036a44d4346a7\|Ch 1.2wcc\|Tue Jul 24 12:57:37 2007 UTC |
| 53b8b9f779b1d1d298884d1c21313ab3\|Ch 1.2wcc\|Tue Jul 24 12:57:37 2007 UTC |
| 69ae46fedf3c18ff36fc850e0baa9365\|Ch 1.2wcc\|Tue Jul 24 12:57:37 2007 UTC |
| e05511a84eb345954b94f1e05c78bf22\|Ch 1.2\|Thu Jul 26 07:20:17 2007 UTC |
| f93ce76f6580d68a95260198b2d6feaa\|Ch 1.3\|Mon Dec 3 14:15:58 2007 UTC |
| db5d1583704b0fb6d1cff0b62a512a7d\|Ch 1.4\|Tue Dec 11 17:36:03 2007 UTC |
| 2b348c225985679f62e50b28bdb74ac9\|Ch 1.4\|Tue Dec 11 17:36:03 2007 UTC |
| af3f0efbd69905123f7df958cc88dff9\|Ch 1.4\|Tue Dec 11 17:36:03 2007 UTC |
| e825c4961293ad45883cd52f38695283\|Ch 1.5\|Thu Mar 27 14:58:15 2008 UTC |
| 2a67b53b7ef7b70763658ca7f60e7005\|Ch 1.5\|Thu Mar 27 14:58:15 2008 UTC |
| bbf569176ec7ec611d8a000b50cdb754\|Ch 1.5\|Thu Mar 27 14:58:15 2008 UTC |
| e5c76e67128e48cb0f003c2beee47d1f\|Ch 1.5\|Thu Mar 27 14:58:15 2008 UTC |
| 8e5da63369d20e1d2c530bf806996285\|Ch 2.02\|Mon May 5 11:27:48 2008 UTC |
| 78d3f074b70788897ae7e20e5137bf47\|Ch 2.03\|Mon May 12 11:52:31 2008 UTC |
| 986f263ca2c529d5d28bce3c62f858ea\|Ch 2.03\|Thu May 22 10:24:55 2008 UTC |
| 4f732099caf5d21729572cec229f7614\|Ch 2.04\|Mon Jun 9 17:23:56 2008 UTC |
| 5336c24a3399f522f8e19d9c54a069c6\|Ch 2.04\|Mon Jun 9 17:23:56 2008 UTC |
| dc1c54751f94b6fdf0b6ecdd64e67701\|Ch 2.04\|Mon Jun 9 17:23:56 2008 UTC |
| 40335fca60acd05f1428b13a9a3c1228\|Ch 2.04\|Mon Jun 9 17:23:56 2008 UTC |
| 72663ee9d3efaff959bff4ce25bd37a6\|Ch 2.04\|Mon Jun 9 17:23:56 2008 UTC |

| |
|---|
| 5ef72904221aa4090a262a24714054f0\|Ch 2.04\|Mon Jun 9 17:23:56 2008 UTC |
| 331eca9c7d9fd9cbe7cd192af09880a3\|Ch 2.05\|Thu Nov 6 13:21:45 2008 UTC |
| db1156b072d58acdac1aeab9af2160a2\|Ch 2.05\|Thu Nov 6 13:21:45 2008 UTC |
| 74dbea70bfb15db31bb9f757ed4bb1a0\|Ch 2.07\|Mon Dec 29 11:37:17 2008 UTC |
| eb928bca5675722c7e9e2b09eec1158a\|Ch 2.07\|Mon Dec 29 11:37:17 2008 UTC |
| 162f415abad9708aa61db8e03bcf2f3c\|Ch 2.11\|Mon Sep 14 13:22:57 2009 UTC |
| 448524fd62dec1151c75b55b86587784\|Ch 2.11\|Mon Sep 14 15:28:07 2009 UTC |
| 29bb70a40689e9e665d15716519bacfd\|Ch 2.12\|Tue Sep 29 10:28:40 2009 UTC |
| 38d6719d6a266c6cefb8626c57378927\|Ch 2.13\|Mon Dec 7 14:25:12 2009 UTC |
| 02eda1effde92bdf8462abcf40c4f776\|Ch 2.13\|Mon Dec 7 14:27:53 2009 UTC |
| 5121ce1f96d74076df1c39748e019f42\|Ch 2.14.1\|Wed Feb 17 15:14:20 2010 UTC |
| 28dc1ca683d6a14d0d1794a68c477604\|Ch 3.00\|Tue Jan 31 16:12:25 2012 UTC |
| 40bd7846553550f38e458b8493824cb4\|Ch 3.00\|Tue Feb 14 10:28:06 2012 UTC |
| ba0c777317461ed57a85ffae277044dc\|Ch 3.02\|Wed Apr 4 16:23:44 2012 UTC |
| b86137fa5a232c614ec5405be4d13b37\|Ch 3.10\|Tue Dec 18 08:22:43 2012 UTC |
| 7872c1d88fe21d8a85f160a6666c76e8\|Ch 3.20\|Fri Jun 28 12:16:40 2013 UTC |
| 83a48760e92bf30961b4a943d3095b0a\|Ch 3.20\|Fri Jun 28 12:16:58 2013 UTC |
| 3d65c18d09f47547f85c631ebeeda482\|Ch 3.20\|Mon Jun 24 10:51:01 2013 UTC |
| ec7e3cfaeaac0401316d66e964be684e\|Ch 3.25\|Thu Feb 6 12:37:44 2014 UTC |
| b407b6e5b4046da226d6e189a67f62ca\|Ch 3.26\|Thu Jan 3 18:03:46 2013 UTC |

Aus den Versionsbezeichnungen können wir ableiten, dass die ermittelten Kompilierungsdaten korrekt sind, mit Ausnahme der letzten bekannten Version, bei der der Entwickler das Kompilierungsdatum modifiziert hat, um die Analyse zu erschweren. Wir sehen, dass diese Malware in den Jahren 2007 und 2008 sehr aktiv war. Weniger neue Versionen wurden im Jahr 2009 veröffentlicht; lediglich ein neues Sample wurde im Jahr 2010 erfasst. Ab dem Jahr 2011 fanden wir keine neuen Samples, aber die Malware tauchte im Jahr 2012 wieder mit einer neuen Hauptversion auf.

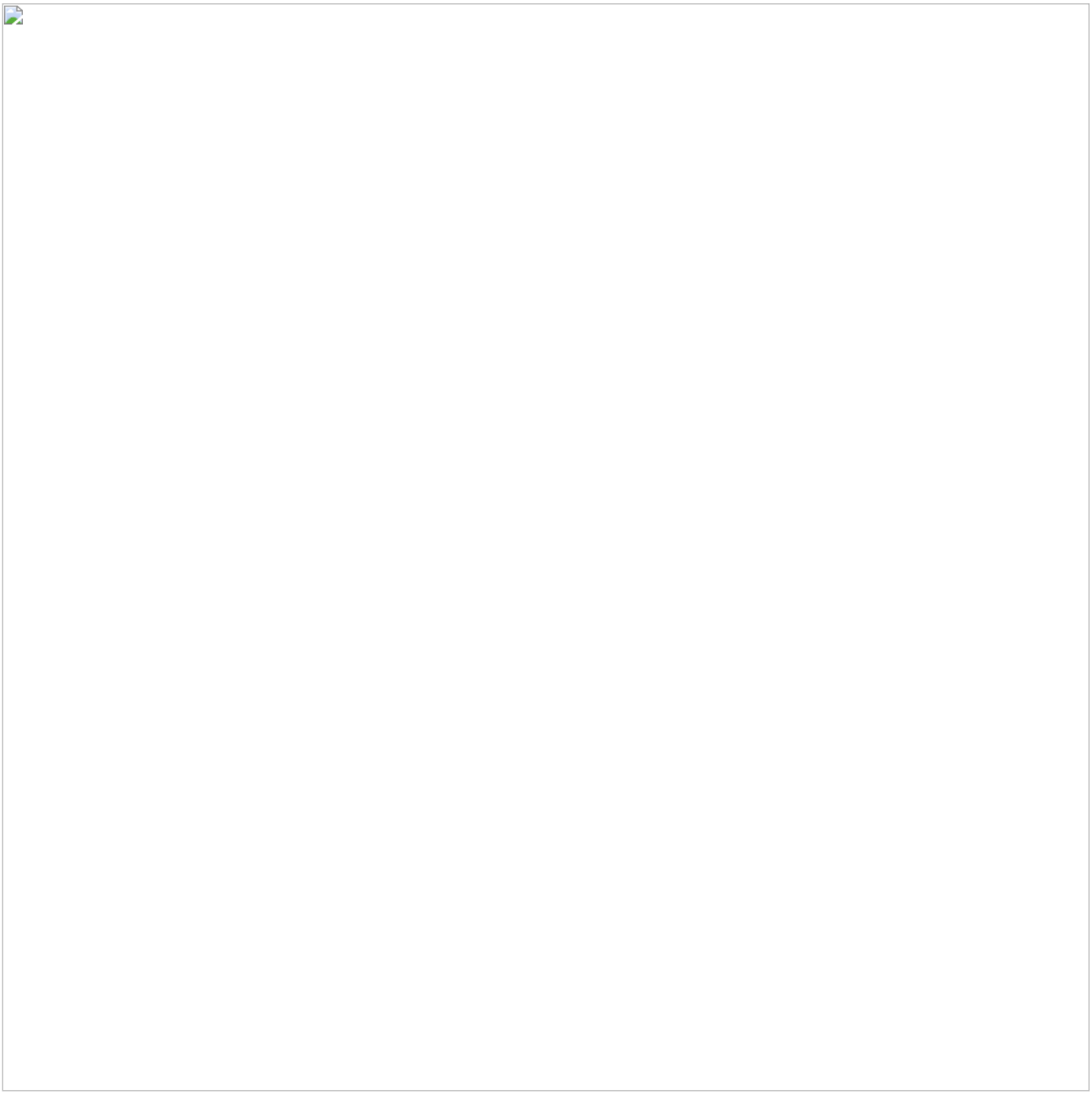


### Die Entwicklung des Fernsteuerungstools in zehn Schritten

Um die Weiterentwicklung der Software zu beschreiben, haben wir zehn Hauptversionen verglichen:

- Version Ch 1.0 (2007-06) im Vergleich zu Ch 1.5 (2008-03)
- Version Ch 1.5 (2008-03) im Vergleich zu Ch 2.03 (2008-05)
- Version Ch 2.03 (2008-05) im Vergleich zu Ch 2.11 (2009-09)
- Version Ch 2.11 (2009-09) im Vergleich zu Ch 2.14.1 (2010-02)
- Version Ch 2.14.1 (2010-02) im Vergleich zu Ch 3.00 (2012-01)
- Version Ch 3.00 (2012-01) im Vergleich zu Ch 3.10 (2012-12)
- Version Ch 3.10 (2012-12) im Vergleich zu Ch 3.20 (2013-06)
- Version Ch 3.20 (2013-06) im Vergleich zu Ch 3.25 (2014-02)
- Version Ch 3.25 (2014-02) im Vergleich zu Ch 3.26 (2013-01; Datum wurde modifiziert)

Im folgenden Kapitel werden die wesentlichen Unterschiede zwischen den oben genannten Versionen dargelegt. Die folgende Tabelle zeigt die Ähnlichkeit der einzelnen Versionen in Prozent; verglichen werden jeweils nur die direkt aufeinanderfolgenden Versionen unter Verwendung von BinDiff:



Die größten Code-Unterschiede sind zwischen Version 2.14.1 und Version 3.00 festzustellen. Dieser Sprung ergibt sich aus dem Fehlen von Samples in den dazwischenliegenden zwei Jahren; diese grundlegende Veränderung bezeichnen wir als das Ende von Agent.BTZ und den Beginn von ComRAT.

## Unterschiede zwischen den Versionen Ch 1.0 (2007-06) und Ch 1.5 (2008-03)

Die analysierten Samples sind folgende:

- Ch 1.0: b41fbdd02e4d54b4bc28eda99a8c1502
- Ch 1.5: bbf569176ec7ec611d8a000b50cdb754
- Ähnlichkeit des Codes: 90 %

Wir haben keine grundlegenden Unterschiede zwischen den beiden Samples feststellen können. Jedoch können wir Folgendes festhalten:

- Die Konfigurationsdatei (XML) in Version 1.5 ist nicht mehr im ASCII-Format, sondern in Unicode gespeichert.
- Beide Versionen implementieren einen Mechanismus, um neue Datenträger zu infizieren, die am infizierten System angeschlossen werden. Weder die Implementierung noch das Protokoll der Datenträgerinfizierung sind identisch.
- Version 1.5 erstellt das neue Event „wowmgr_is_load“. Dieses Event wurde dann jahrelang verwendet.

## Unterschiede zwischen den Versionen Ch 1.5 (2008-03) und Ch 2.03 (2008-05)

Die analysierten Muster sind folgende:

- Ch 1.5: bbf569176ec7ec611d8a000b50cdb754
- Ch 2.03: 78d3f074b70788897ae7e20e5137bf47
- Ähnlichkeit des Codes: 83 %

In Version 2.03 von Agent.BTZ haben die Entwickler Folgendes geändert:

- Sie führten eine Verschlüsselungstechnik ein, um kritische Zeichenketten zu verbergen.
- Dem Kommunikationsprotokoll wurde das Flag „<CHCMD>“ hinzugefügt.

Wir gehen davon aus, dass „CH“ dieselbe Bedeutung wie „Ch“ vor der Versionsnummer hat und „CMD“ eine Abkürzung für Command (Befehl) ist.

> Von nun an unterstützt die Malware „Runas“, um Befehle als Administrator auszuführen. Dieser Befehl wurde im Jahr 2007 von Microsoft in Windows Vista implementiert. Wir gehen davon aus, dass der Entwickler diese Funktion implementiert hat, weil mehrere Zielcomputer im Jahr 2008 auf diese Windows-Version umstiegen.

Laut einem Bericht wurde Version 1.5 für einen Angriff gegen das US-Verteidigungsministerium (Pentagon) eingesetzt. Wir gehen davon aus, dass die Zeichenfolgenverschlüsselung durchgeführt wurde, um Sicherheitsmaßnahmen zu umgehen, die Angriffe erkennen sollen.

## Unterschiede zwischen den Versionen Ch 2.03 (2008-05) und Ch 2.11 (2009-09)

Die analysierten Muster sind folgende:

- Ch 2.03: 78d3f074b70788897ae7e20e5137bf47
- Ch 2.11: 162f415abad9708aa61db8e03bcf2f3c
- Ähnlichkeit des Codes: 96 %

Der Programmcode dieser beiden Versionen weist kaum Unterschiede auf. Wir konnten nur sehr geringe Unterschiede feststellen:

- Der Entwickler hat die Bezeichnung mehrerer Registry-Schlüssel geändert (vermutlich, um die Erkennung durch bekannte IOCs zu vermeiden).
- Auch die Bezeichnungen zweier exportierter Funktionen wurden geändert: Aus InstallM() wurde AddAtomT() und aus InstallS() wurde AddAtomS(), wahrscheinlich aus denselben, bereits oben dargelegten Gründen.

## Unterschiede zwischen den Versionen Ch 2.11 (2009-09) und Ch 2.14.1 (2010-02)

Die analysierten Muster sind folgende:

- Ch 2.11: 162f415abad9708aa61db8e03bcf2f3c
- Ch 2.14.1: 5121ce1f96d74076df1c39748e019f42
- Ähnlichkeit des Codes: 98 %

Auch bei diesen Versionen ist der Code sehr ähnlich. Wir konnten nur zwei Unterschiede feststellen:

- Der Entwickler hat einige Fehler gepatcht.
- Es sind vier neue Exporte vorhanden: DllCanUnLoadNow(), DllGetClassObject(), DllRegisterServer(), DllUnregisterServer().

Die vier exportierten Bibliotheken zeigen, dass die Malware erstmalig das OLE Component Object Model (COM) unterstützt. Diese Version ist die erste Version, die in der Lage ist, als COM-Objekt registriert zu werden. Drei der vier Funktionen haben keinen Inhalt. Die vierte Funktion führt die Malware aus.

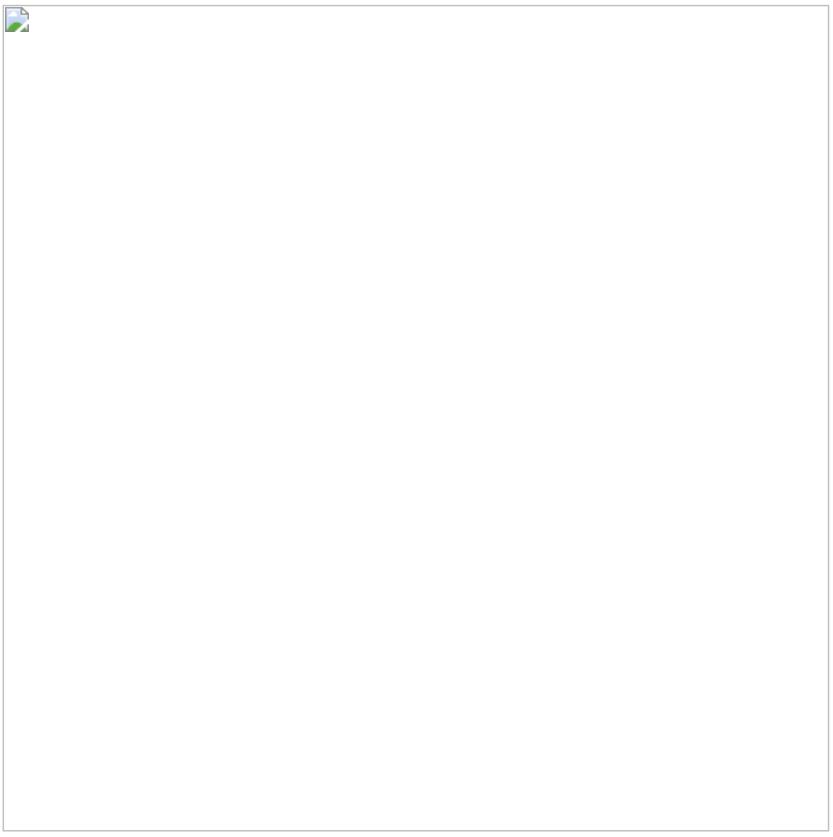
## Unterschiede zwischen den Versionen 2.14.1 (2010-02) und Ch 3.00 (2012-01)

Die analysierten Muster sind folgende:

- Ch 2.14.1: 5121ce1f96d74076df1c39748e019f42
- Ch 3.00: 28dc1ca683d6a14d0d1794a68c477604
- Ähnlichkeit des Codes: 60 %

Der Code dieser Versionen weist große Unterschiede auf, wenngleich einige Teile von Version 2.14.1 beibehalten wurden. Außerdem haben die Entwickler einen anderen Compiler benutzt; sie sind von Visual Studio 6.0 auf Visual Studio 9.0/10.0 umgestiegen, was ein bedeutender Indikator für die großen Unterschiede ist.
Version 3.00 ist die Version, die die Experten der G DATA SecurityLabs als „ComRAT“ bezeichnen. Damit ist Version 2.14.1 die letzte Version von Agent.BTZ. Hier die wichtigsten Unterschiede zwischen Agent.BTZ und ComRAT:

- Die neue Malware sammelt mehr Informationen über das infizierte System (beispielsweise Laufwerksinformationen, Volume-Informationen usw.)
- Der Mechanismus zum Infizieren von Datenträger-Sticks wurde endgültig entfernt. Der Grund hierfür ist vermutlich, dass Microsoft die automatische Ausführung bei externen Datenträgern deaktiviert hat. Für die Angreifer ist dieser Infektionsvektor nicht mehr interessant.
- Die Malware wird in jeden Prozess des infizierten Computers injiziert; die primäre Payload wird in „explorer.exe“ ausgeführt, wie wir in unserem Bericht "Die Akte Uroburos: neues, ausgeklügeltes RAT identifiziert" erläutert haben.
- Der Kommunikationskanal zum Command & Control Server ist nicht mehr derselbe. In der neuen Version nutzt die Malware POST-Anfragen nach folgendem Muster:



Da die Malware in jeden Prozess des infizierten Systems injiziert wird, erstellt sie eine sogenannte „Named Pipe“ für die prozessübergreifende Kommunikation.

Bei mehreren Samples von Version 3.00 vergaß der Entwickler, den Kompilierungspfad zu entfernen. Hier einige Beispiele:

- c:\projects\ChinckSkx64\Debug\Chinch.pdb
- c:\projects\ChinckSkx64\Release\libadcodec.pdb
- C:\projects\ChinckSkx64\x64\Release\libadcodec.pdb
- E:\old_comp_Chinch\Chinch\trunk\Debug\Chinch.pdb
- c:\projects\ChinchSk\Release\libadcodec.pdb

Aufgrund dieser Kompilierungspfade gehen wir davon aus, dass der ursprüngliche Name des Fernsteuerungstools „Chinch“ ist. Dies führt uns zu der Annahme, dass die Zeichenfolge „CH“ in der Versionsbezeichnung und im Flag „<CHCMD>“ für „Chinch“ steht. Das englische Wort „Chinch“ bezeichnet das kleine nordamerikanische Insekt mit der wissenschaftlichen Bezeichnung Blissus leucopterus. Dieses Wort leitet sich vom spanischen Wort „chinche“ ab, das Wanze bedeutet.

## Unterschiede zwischen den Versionen Ch 3.00 (2012-01) und Ch 3.10 (2012-12)

Die analysierten Muster sind folgende:

- Ch 3.00: 28dc1ca683d6a14d0d1794a68c477604
- Ch 3.10: b86137fa5a232c614ec5405be4d13b37
- Ähnlichkeit des Codes: 90 %

Der Code ist bei diesen Versionen ähnlich, doch die Entwickler haben einige neue Funktionen integriert:

- Die Malware generiert mehr Protokolle.
- Die Malware verfügt über einen Mutex-Handle.
- Version 3.10 unterstützt mehrere Command & Control Server.

Diese letztgenannte neue Funktion ist sehr interessant: Wenn die kompromittierten Zielcomputer einen bestimmten C&C-Server blockieren, funktioniert die Malware dennoch weiterhin über zwei alternative Command & Control Server.

## Unterschiede zwischen den Versionen Ch 3.10 (2012-12) und Ch 3.20 (2013-06)

Die analysierten Samples sind folgende:

- Ch 3.10: b86137fa5a232c614ec5405be4d13b37
- Ch 3.20: 7872c1d88fe21d8a85f160a6666c76e8
- Ähnlichkeit des Codes: 93 %

Die wichtigste neue Funktion dieser Version ist die neue Exportfunktion InstallW(). Diese Exportfunktion wird vom Dropper dazu verwendet, dauerhafte Registry-Einträge zu erstellen und – wie in unserem letzten Artikel beschrieben – eine zweite Datei abzusetzen. Version 3.20 verwendet die folgende CLSID, um ein COM-Objekt zu manipulieren: B196B286-BAB4-101A-B69C-00AA00341D07. Dieses Objekt ist die Schnittstelle IConnectionPoint. Die CLSID wurde nur in dieser Version verwendet.

Wir gehen davon aus, dass die durchgeführte Manipulation des COM-Objekts einige Probleme auf dem infizierten System erzeugt. Deshalb hat der Entwickler damit im Zusammenhang stehende Aspekte in der nächsten Version geändert. Darüber hinaus wurde die CLSID im Sample in Klartext gespeichert.

## Unterschiede zwischen den Versionen Ch 3.20 (2013-06) und Ch 3.25 (2014-02)

Die analysierten Samples sind folgende:

- Ch 3.20: 7872c1d88fe21d8a85f160a6666c76e8
- Ch 3.25: ec7e3cfaeaac0401316d66e964be684e
- Ähnlichkeit des Codes: 91 %

In Version 3.25 ist der Entwickler auf folgende CLSID umgestiegen: 42aedc87-2188-41fd-b9a3-0c966feabec1. Dies wird in unserem Bericht "Die Akte Uroburos: neues, ausgeklügeltes RAT identifiziert" beschrieben. Zudem sind die Zeichenketten im Muster verschlüsselt. Die wichtigste Neuerung ist die Verschlüsselung – fast alle Zeichenketten sind verschlüsselt, und das XML-Muster ist nicht mehr in Klartext geschrieben.

## Unterschiede zwischen den Versionen 3.25 Ch (2014-02) und Ch 3.26 (2013-01; Datum wurde modifiziert)

Die analysierten Samples sind folgende:

- Ch 3.25: ec7e3cfaeaac0401316d66e964be684e
- Ch 3.26: b407b6e5b4046da226d6e189a67f62ca

- Ähnlichkeit des Codes: 95 %

Version 3.26 ist die jüngste bekannte Version. In dieser Version haben die Entwickler folgende Änderungen vorgenommen:

> Der bekannte, in Agent.BTZ und Uroburos genutzte, XOR-Schlüssel wurde entfernt. Wir gehen davon aus, dass sich der Entwickler aufgrund der G DATA-Veröffentlichung im Februar 2014 dazu entschlossen hat, möglichst viele Zusammenhänge zwischen Uroburos und Agent.BTZ/ComRAT/Chinch zu entfernen.

- Die Entwickler generieren keine Protokolle mehr.
- Das Kompilierungsdatum wurde geändert, um die Analyse und die Erstellung einer Zeitleiste zu erschweren.

## Fazit

Diese Analyse zeigt uns die Entwicklung eines Fernsteuerungstools über sieben Jahre. Es wird von einer Gruppe genutzt, die Angriffe gegen sensible Organisationen wie etwa im Jahr 2008 gegen das US-Verteidigungsministerium (Pentagon) oder im Jahr 2014 gegen das belgische Außenministerium sowie gegen das finnische Außenministerium richtete.

Bis auf die Änderungen in Version 3.00 sind die vorgenommenen Änderungen eher marginal. Wir erkennen, dass die Entwickler Funktionen an die Windows-Versionen angepasst, Fehler gepatcht, Verschlüsselungstechniken integriert haben usw. Das größte Update auf Version 3.00 wurde nach zwei Jahren des Schweigens durchgeführt. Offenbar wurde dieses Fernsteuerungstool parallel zum Uroburos-Rootkit eingesetzt. Dennoch ist nicht völlig klar, wie und wann die Angreifer sich dazu entschieden haben, das Fernsteuerungstool oder das Rootkit einzusetzen oder ob beide Tools parallel genutzt werden.

Unter Berücksichtigung aller Aspekte sind die Experten der G DATA SecurityLabs davon überzeugt, dass die Gruppe, die hinter Uroburos/Agent.BTZ/ComRAT bzw. dem Linux-Tool steckt, auch weiterhin eine aktive Rolle im Bereich Malware und APT spielen wird. Aufgrund der neuesten Analyseergebnisse und der daraus gezogenen Schlussfolgerungen kommen wir zu der Ansicht, dass noch weitere Bedrohungen folgen werden.